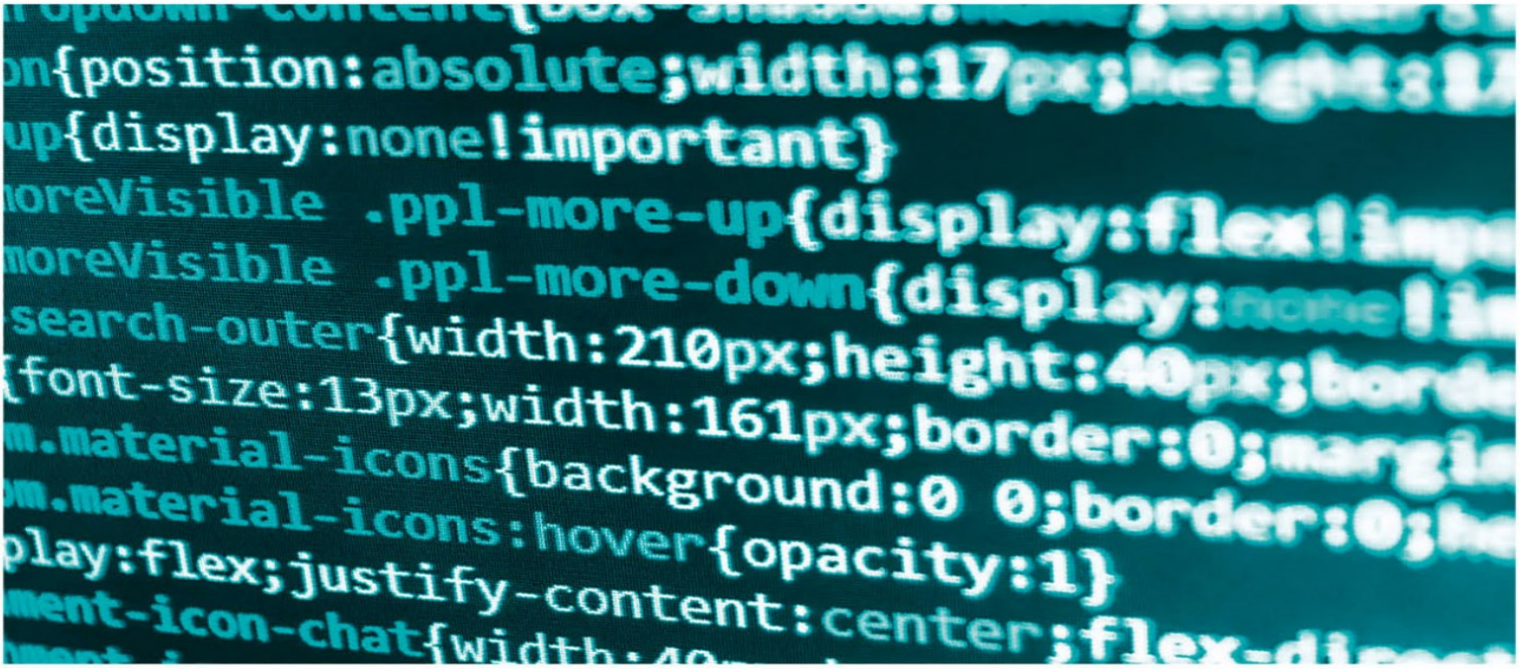

PIERRE PHILIPPE
GASTINEAU VASSET

ARMES DE DÉSTABILISATION MASSIVE

Enquête sur le business des fuites de données

fayard

Philippe Vasset Pierre Gastineau

Armes de déstabilisation massive

Fayard

“People love to talk about the technology, but our greatest edge isn’t technology; our greatest edge is that motivated man or woman with the intellectual capacity to anticipate, to be innovative and to be agile. Because… what we’re dealing with is driven by a man or woman somewhere in the world sitting at a keyboard. There’s a human dimension in all of this. It’s not just about the machine[1].”
Amiral Mike Rogers, commandant du Cyber Command américain et directeur de la National Security Agency.

Prologue

Le 22 juillet 2016, à trois mois de l'élection présidentielle américaine, le site WikiLeaks met en ligne un dossier rassemblant 20 000 e-mails internes du Parti démocrate.

Le 6 mai 2017, un fichier regroupant les messageries de plusieurs conseillers d'Emmanuel Macron est posté sur le forum 4chan, à deux jours du second tour de l'élection présidentielle française.

Aucune de ces deux publications ne révèle de scandales majeurs : ce sont, pour l'essentiel, des reliefs de campagne présidentielle, des comptabilisations de donations, des recherches de soutien, des propositions de loi, des listes de nominations potentielles et les inévitables blagues, parfois de mauvais goût. Des informations intéressantes, certes, mais en aucun cas dévastatrices.

Pourtant, leur mode de diffusion va jeter le soupçon sur les candidats visés : si la correspondance des partisans de Hillary Clinton et d'Emmanuel Macron se retrouve sur la place publique, n'est-ce pas le signe que les deux candidats ont quelque chose à cacher ? Claironnée par des milliers d'internautes relayant les bannières DNCLeak et Macronleaks, cette vérité s'impose bientôt, et pèse sur le scrutin.

En France, l'opération, trop brouillonne, échoue : Emmanuel Macron est élu haut la main le 8 mai. Mais, aux États-Unis, le contenu des mails piratés empoisonne durablement la campagne de Hillary Clinton et bénéficie à son adversaire, le républicain Donald Trump, élu le 8 novembre 2016.

Ces deux fichiers piratés, diffusés pour faire dérailler les deux présidentielles, suscitent un électrochoc dans les sociétés occidentales. Jusqu'ici accros aux « leaks », ces fuites massives et anonymes d'informations confidentielles, les médias opèrent une spectaculaire volte-face et commencent à s'interroger sur l'origine des fuites, ce qu'ils avaient obstinément refusé de faire lorsque WikiLeaks – encore lui ! – avait publié,

en 2010, près de 251 287 télégrammes diplomatiques américains, ou lorsque « John Doe », un informateur anonyme, lui avait fourni près de 11,5 millions d'e-mails et actes d'incorporation du cabinet panaméen Mossack Fonseca. Mieux, journaux et télévisions parlent pour la première fois de « piratage », terme qu'aucun d'entre eux n'avait employé jusque-là.

Le piratage, donc, du Parti démocrate américain et du mouvement En marche ! d'Emmanuel Macron a constitué un tournant : la prise de conscience que les fuites massives de données ne sont pas seulement des initiatives désintéressées de lanceurs d'alerte courageux, mais également des techniques de manipulation, voire des armes de déstabilisation massive. C'est ce phénomène que ce livre voudrait creuser, et étayer.

Car, en dix ans, la fuite de bases de données numériques est devenue un phénomène à part entière, un genre, presque une marque. Depuis que le site cryptome.org a publié, en 2005, les noms de 276 agents du MI6, le service de renseignement extérieur britannique, on ne compte pas moins de trente-cinq publications non autorisées, et souvent illégales, de fichiers protégés sur Internet (on trouvera un recensement complet en fin de volume).

Certains cas sont célèbres : les archives de la National Security Agency volées, puis transmises par Edward Snowden à plusieurs journalistes, ont transformé l'ancien ingénieur réseau du renseignement américain en célébrité planétaire. D'autres le sont moins : qui, hors de France, sait que la messagerie personnelle de l'ancien directeur du Renseignement intérieur, Bernard Squarcini, a fuité sur un obscur site kazakh ? Qui, hors du cercle étroit des pénalistes de la City, sait que le promoteur Dar al-Arkan, géant de l'immobilier du Golfe, a nourri le vaste procès engagé contre l'un de ses directeurs grâce aux e-mails de ce dernier, miraculeusement apparus sur Internet ?

Si différentes soient-elles, toutes ces fuites suivent le même scénario, rodé comme le lancement d'un nouveau modèle de téléphone ou d'un blockbuster américain :

1 – Un opérateur anonyme met en ligne, ou bien confie à des journalistes, une masse considérable de données subtilisées sur les serveurs internes d'une entreprise ou d'une administration.

2 – Les journalistes se réunissent en consortium pour éplucher les nombreuses informations reçues et écrire des articles, souvent publiés pendant plusieurs jours ou semaines.

3 – Les propriétaires des documents originaux crient au vol ou à la trahison.

4 – La publication des données suscite des démissions, des enquêtes judiciaires, voire des coups de théâtre électoraux, jusqu'au prochain épisode.

Plusieurs caractéristiques majeures différencient les fuites massives des révélations traditionnellement relayées par la presse :

1 – Grâce aux facilités offertes par les technologies de l'information, ces opérations portent sur des bases de milliers, voire de millions de données.

2 – Les contenus diffusés sont toujours authentiques, ce qui en démultiplie la portée.

3 – Les révélations sont nimbées d'une véritable mythologie, capturée par les films *Snowden* d'Oliver Stone et *Le Cinquième Pouvoir* de Bill Condon, qui mettent en scène de courageux lanceurs d'alerte scandalisés par les abus de pouvoir perpétrés par des administrations secrètes décidées à les faire taire.

Nous avons tenté d'aller au-delà de la mythologie pour répondre à quelques questions simples : pourquoi assiste-t-on à une généralisation des fuites massives depuis une décennie ? Quelles sont les coulisses de ces opérations ? Qui est à la manœuvre, et surtout à qui bénéficient-elles ?

Pour y répondre, nous avons procédé à l'ancienne, en allant, carnet en main, rencontrer les principaux acteurs de ce secteur en pleine expansion. Par scepticisme, incontestablement, par esprit de contradiction, sans doute, mais surtout par souci de vérité. Car les fuites massives, on l'a dit, sont paramétrées pour être anonymes : les chances de remonter à la source sont quasiment nulles si l'on se cantonne à l'examen des données et métadonnées contenues dans les fichiers disséminés.

Pour prendre l’ampleur du phénomène, et surtout comprendre comment il fonctionne, nous sommes allés à la rencontre des professionnels des « leaks » qui prospèrent dans l’ombre : les hackers qui piratent les messageries ; les agents de renseignement, initialement dépassés par le phénomène, mais qui, aujourd’hui, commanditent parfois les vols de données ; les enquêteurs privés et les avocats qui utilisent cette technique pour le compte des multinationales ; les sites Internet et les journaux qui relaient les documents subtilisés ; et les enquêteurs informatiques chargés d’empêcher tout ce beau monde d’agir.

Puisque la fuite massive est désormais un véritable secteur d’activité, nous avons choisi d’organiser notre enquête autour des principaux métiers qui participent de son essor, en commençant par les plus opérationnels, à savoir les professionnels de l’intrusion des réseaux, pour poursuivre avec les donneurs d’ordres, qu’ils s’agissent d’États ou d’entreprises, et finir avec tous ceux qui, sur la toile ou dans les kiosques, diffusent les bases de données illégalement obtenues.

Si certains praticiens ont accepté – avec réticence – de témoigner, beaucoup nous ont fermé la porte au nez, parfois violemment. Le vol et la diffusion de données confidentielles restent un délit dans presque toutes les juridictions du globe et, dans la très secrète communauté de la fuite massive, il n’existe pas de bonne publicité.

Au cours de cette longue enquête, qui nous a menés de Tel Aviv à Zurich et New York en passant par Londres et Genève, la comparaison avec la guerre froide s’est petit à petit imposée. Nous pensions pénétrer dans un monde glacé, fait d’échanges désincarnés, mais nous avons découvert, à l’inverse, un univers où la manipulation des individus compte davantage que celle des données. Les tacticiens de la fuite massive consacrent plus de temps à séduire, mentir et menacer leurs cibles, leurs sources et les pirates informatiques qu’ils emploient qu’à chercher des voies d’accès dans les messageries. La bataille des réseaux n’est pas autre chose qu’une guerre de position, un affrontement par personnes interposées, jouant sur l’ambition, l’orgueil et la cupidité des uns et des autres.

Si certaines fuites massives sont, sans conteste, l’œuvre de lanceurs d’alerte désintéressés qui ont pris des risques considérables pour révéler des

informations qu’ils jugeaient choquantes, ces épisodes constituent, dans la grande parade des « leaks », une minorité.

Le soldat Bradley Manning qui, en 2009, a transmis à WikiLeaks quatre années de télégrammes diplomatiques américains et a écopé d’une condamnation à trente-cinq ans de prison, n’avait d’autres motivations que la dénonciation des opérations américaines en Irak. Même constat pour Antoine Deltour et Raphaël Halet, les deux consultants de PriceWaterhouseCoopers à l’origine de la fuite des données fiscales des grands groupes installés au Luxembourg (LuxLeaks).

Mais ces quelques fuites « pures » ont tendance à éclipser toutes les autres, dont les motivations sont bien plus troubles. De plus en plus, on trouve des oligarques, des entreprises et des gouvernements derrière les « leaks » les plus médiatisés. Tous se sont saisis de cette nouvelle technique pour mener leurs guerres diplomatiques, commerciales ou médiatiques. Des campagnes menées sur Internet, bien sûr, mais surtout dans les esprits des fantassins de ces batailles numériques mondiales, aiguillés, orientés, menacés, pourchassés par des marionnettistes qui n’ont rien à envier aux maîtres espions de l’ex-URSS ou de l’Amérique de Kennedy.

Dans cet univers de glaces sans tain et de faux-semblants, toute entreprise de vérité est de longue haleine. Démasquer l’auteur d’une fuite massive s’est révélé plus ardu que d’établir qui, dans les années 1970, se cachait derrière tel groupe terroriste ou tel mouvement de guérilla. Pour éviter que les hypothèses ne deviennent des certitudes et que notre enquête ne bascule dans la théorie du complot, nous avons pris soin de toujours indiquer nos doutes, nos suppositions et, parfois, nos impasses. L’économie de la fuite prospère sur la fiction : nous ne voulions pas rajouter des rebondissements à un feuilleton déjà riche en épisodes imaginaires.

La matière éminemment volatile de cette enquête a également conditionné sa mise en forme. Plutôt que d’asséner des histoires dont la reconstitution nous a pris des mois, nous avons préféré partager nos voyages, nos doutes, nos dîners trop arrosés et nos bisbilles de co-auteurs. Vérifiez vos connexions réseau et changez tous vos mots de passe : bienvenue dans les cyber-tranchées !

I

Les intrigants

Paris, février 2015. « Vous avez vu ce site, Kazaword ? » Notre interlocuteur est plein de sollicitude : il veut nous aider. « Vraiment, vous devriez jeter un œil : il y a plein d'histoires pour vous. » Lorsque nous nous connectons, le site n'a presque jamais été consulté, et ce, bien qu'il soit en ligne depuis plusieurs mois. La mise en page est sommaire, une architecture Wordpress qui rappelle les premiers blogs des années 1990, avec, bien visible en haut de la page, un dossier à télécharger. Nous nous exécutons : à l'intérieur, près de quatre ans de correspondance de Jean Galiev, le ministre-conseiller de l'ambassade kazakhe en France. Éponge à pétrole et à gaz dirigée d'une main de fer par Nursultan Nazarbayev depuis trente ans, le Kazakhstan est un émirat de bande dessinée où les contrats se chiffrent en milliards de dollars et les disgrâces présidentielles en années de prison. Pays de cocagne pour les intrigants de tout poil, c'est une source presque inépuisable d'histoires aussi rocambolesques que violentes.

L'une de ces sagas ne tarde pas à apparaître dans les mails piratés : celle de Mukhtar Ablyazov, un richissime homme d'affaires longtemps proche de la présidence kazakhe, qui s'est vu accusé en 2009 de détournements totalisant près de 3 milliards de dollars. En cavale à travers toute l'Europe, une armée d'enquêteurs privés à ses trousses, il a été arrêté en juillet 2013 sur la Côte d'Azur. Visé par un mandat Interpol, l'oligarque croupit depuis dans les prisons françaises, en attendant une hypothétique extradition.

Règlement de comptes intra-kazakh, l'affaire questionne les autorités françaises. Aussi riche que déterminé, l'oligarque traqué se présente comme un opposant au très autoritaire régime de Nursultan Nazarbayev. Mais cet autoportrait de circonstance n'est qu'imparfaitement fidèle : Mukhtar Ablyazov a été l'un des ministres du président Nazarbayev et a dirigé la

BTA, principale banque du pays : un poste que l'on n'obtient pas en critiquant le régime…

Au flou sur le personnage vient s'ajouter une situation diplomatique pour le moins délicate : le Kazakhstan est un fidèle client de l'industrie française, notamment dans le domaine militaire. C'est aussi l'un des pays où la société nucléaire Areva extrait une partie de son uranium. Un client à ne pas froisser, donc, si autocratique soit-il.

Ablyazov arrêté, la machine judiciaire française se met en branle pour l'extrader au plus vite. Non vers le Kazakhstan, avec lequel Paris n'a pas de traité de coopération judiciaire, mais vers la Russie et l'Ukraine, deux fidèles alliés d'Astana. Que feront Kiev et Moscou du fugitif une fois qu'ils l'auront récupéré ? Pour les avocats d'Ablyazov, la réponse ne fait aucun doute : ils le livreront au Kazakhstan, où il sera probablement exécuté. Deux mois plus tôt, l'Italie a déjà arrêté la femme et la fille de l'oligarque et les a renvoyées au Kazakhstan sans autre forme de procès. Il a fallu que des députés italiens protestent contre ce « kidnapping » au Parlement pour que la famille d'Ablyazov revienne à Rome.

C'est à ce moment critique, en février 2015, que les mystérieux e-mails nous sont aimablement signalés. À leur lecture, on découvre que le Kazakhstan pèse de tout son poids sur Paris pour accélérer l'extradition d'Ablyazov. L'ambassade du Kazakhstan en France est en contact quasi quotidien avec François Delahousse, sous-directeur Asie centrale au ministère des Affaires étrangères. Pour redorer son image, ternie par les avocats d'Ablyazov, le pays fait feu de tout bois, recrutant des conseilleurs prestigieux tels Jacques Attali ou le banquier Jean Lemierre, et multipliant les contrats de relations publiques avec des agences de communication. Une stratégie d'influence savamment organisée, mais éventée en quelques clics par le piratage et la diffusion massive des messageries de ses agents.

Nous ne sommes pas les seuls à avoir reçu un coup de fil « amical ». Très vite, plusieurs médias français, parmi lesquels Mediapart et *Le Canard enchaîné*, publient le contenu des messages de l'ambassade kazakhe, dénonçant l'extradition « sous influence » d'Ablyazov. Mais la justice française reste inflexible : en première instance, puis en appel, l'oligarque est condamné à être renvoyé hors de France.

*

Londres, mars 2017. Voilà plus de six mois que nous cherchions à le rencontrer. L'homme nous a appelés, la veille, depuis les États-Unis, nous donnant rendez-vous le lendemain dans la capitale anglaise, dans le hall du très victorien Renaissance Hotel. Sortis de l'Eurostar en nage, nous entrons juste à l'heure dans la salle et cherchons parmi les buveurs en costume un profil d'informaticien. Car nous en sommes persuadés, l'homme que nous sommes venus voir est directement mêlé au piratage des boîtes mails de la diplomatie kazakhe. Plusieurs de ses associés et anciens amis nous l'ont assuré, et le principal intéressé n'a accepté de nous rencontrer qu'après un harcèlement en règle.

C'est lui qui nous voit en premier : avenant, musclé, il n'a pas exactement l'allure d'un drogué du clavier. La discussion s'engage prudemment : l'homme reste courtois, mais exige de savoir comment nous l'avons identifié. Sans dévoiler nos sources, nous expliquons que son nom circule beaucoup dans le dossier Ablyazov et que son profil est, pour le moins, digne d'intérêt : vétéran d'une unité de renseignement de l'armée israélienne, notre interlocuteur s'est ensuite reconverti dans l'enquête privée aux États-Unis, avec une prédilection pour les dossiers complexes et âprement disputés. « C'est vrai que j'ai travaillé sur le dossier Ablyazov, reconnaît-il. J'étais mandaté par le Kazakhstan. »

En cercles concentriques, nous reprenons toute l'affaire, pour aboutir au point qui nous intéresse aujourd'hui : le piratage des messageries des hauts fonctionnaires kazakhs. « Je n'ai jamais douté que c'était une opération montée par Ablyazov », explique-t-il. Certes, mais comment trouve-t-on des hackers pour pénétrer dans des messageries gouvernementales quand on est enfermé à la prison de la Santé ?

L'homme nous regarde comme si nous étions légèrement demeurés : « Ce n'est évidemment pas lui qui a monté l'opération ! » Alors qui ? La commisération de notre interlocuteur vire à la pitié : « Mais, sa belle-famille ! La fille d'Ablyazov est mariée au fils de Viktor Khrapunov, l'ancien maire d'Almaty qui vit en exil à Genève, lui aussi en guerre contre le Kazakhstan. »

Si l’on résume : deux oligarques en rupture de ban ont donc monté une campagne de guérilla informatique pour régler leurs comptes avec un État souverain ? « Absolument. » Et qui ont-ils trouvé pour conduire une opération pareille ? « Des professionnels du piratage ! Vous savez, il existe un peu partout des techniciens formés à la pénétration de réseaux par leur gouvernement. Après une période d’active, dans l’armée ou les services de renseignement, ils se reconvertissent dans le conseil et mettent leurs talents aux services d’entreprises ou de pays étrangers, sans couper le lien avec leur maison-mère. Ceux qui ont piraté les boîtes électroniques kazakhes ont ce profil. » Des noms ! « Dans ce milieu-là, être identifié équivaut à une peine de mort… Et puis je ne sais pas tout. Je peux juste vous dire qu’ils sont plusieurs, et qu’ils sont israéliens. »

Nous multiplions les tentatives pour avoir des détails, avançons des noms, dont celui d’un ancien officier qui a pignon sur rue, mais une serveuse vient interrompre ces confidences pour nous demander si nous souhaitons autre chose. Comme mû par un ressort, l’homme jette un coup d’œil à sa montre et se lève brusquement. Nous nous récrions, nous avons tout notre temps, mais il rassemble ses affaires et sort dans la nuit de King’s Cross, non sans nous avoir lâché, droit dans les yeux : « Quoi que vous écriviez, pas question que j’apparaisse ! Je suis trop étroitement mêlé à cette histoire, tout le monde me reconnaîtrait. » Un avertissement qui va très vite devenir une antienne tout au long de notre enquête…

*

Paris, automne 2016. La publication des mails a retardé la procédure d’extradition lancée contre Mukhtar Ablyazov, mais n’a pas entamé la résolution de l’État français. Le gouvernement de Manuel Valls ne fait pas mystère de ses ambitions : l’homme d’affaires doit être renvoyé en Ukraine et ne pas parasiter les efforts de la diplomatie commerciale française en Asie centrale. En septembre 2016, Manuel Valls a signé lui-même le décret d’extradition. Le départ de l’oligarque n’est plus qu’une question de jours.

C’est à ce moment précis que le fameux site Kazaword, resté muet depuis des mois, entre à nouveau en activité. Un nouveau dossier est mis en ligne, là encore accompagné de discrets coups de fil à quelques journalistes-clefs. Dans le dossier, des centaines de mails, tous extraits de la messagerie de

Bernard Squarcini dit le « Squale », omnipotent directeur du renseignement intérieur sous la présidence de Nicolas Sarkozy (2007-2012). Reconverti dans le privé, ce dernier est désormais consultant d'une société d'enquête américaine, Arcanum Global Intelligence, qui compte parmi ses principaux clients… le Kazakhstan !

À la lecture de ses mails, on découvre que l'ex-haut fonctionnaire a joué les petites mains pour faire venir à Paris le ministre de la Justice kazakh Marat Beketayev, et son homologue de la Défense Imangali Tasmagambetov. But du voyage : rencontrer des responsables français et hâter la procédure d'extradition d'Ablyazov, en utilisant le carnet d'adresses de Bernard Squarcini. Grâce à lui, les autorités kazakhes ont pu rencontrer l'ancien député socialiste Julien Dray, ainsi que Laurent Obadia, l'homme des affaires réservées du géant de l'eau Veolia Environnement. La tentative d'influence, là encore, est patente et s'étale à la une des journaux.

*

Zurich, mars 2017. Notre mystérieux témoin a accepté de nous revoir. Il skie en Suisse avant de se rendre en Israël et nous a donné rendez-vous dans une galerie commerciale. L'endroit, banal à souhait, tranche avec les intrigues électroniques internationales qui nous occupent. Nous prenons deux cafés à cinq francs suisses en écoutant la musique d'ascenseur diffusée par les haut-parleurs. « Attendez-moi, je vous trouverai », nous a-t-il dit.

À l'heure dite, l'homme apparaît, toujours charmant, mais toujours sur ses gardes. Depuis notre conversation de Londres, les pistes qu'il nous a distillées tournent en boucle dans nos esprits. Nous lui soumettons de nouveaux noms de hackers israéliens susceptibles d'avoir piraté les messageries kazakhes, ainsi que celle de Bernard Squarcini. Il nous arrête : « Dans le monde souterrain de la piraterie, tout n'est pas aussi simple. Les deux opérations ont été commanditées par le camp Ablyazov, il n'y a aucun doute là-dessus, mais ce ne sont pas les mêmes prestataires qui ont attaqué les fonctionnaires kazakhs et Bernard Squarcini. Les premiers, je vous l'ai dit, sont israéliens. Cependant, le second est indien. » Son nom ? « Je ne connais que son prénom : Rajat. Il faut que vous compreniez que l'Inde est un far west électronique : les Indiens sont très appréciés en matière de piratage, car ils parlent anglais. Contrairement aux Russes, ils ne risquent

pas de laisser des morceaux de codes en cyrillique sur les dossiers qu'ils manipulent. »

Comment notre interlocuteur sait-il que ce Rajat a œuvré pour Ablyazov ? « Ah, ça, c'est facile : il a d'abord proposé de travailler pour notre camp, celui du Kazakhstan ! Un jour, sa secrétaire m'a appelé : il venait d'ouvrir une petite antenne à Genève et se proposait de faire du hacking pour les enquêteurs privés et les avocats ! Je lui ai dit que c'était illégal et de ne plus jamais rappeler ! » Nous échangeons des regards entendus : les professions de vertu de notre interlocuteur sont difficiles à croire… « Quand les e-mails kazakhs ont fuité, j'ai vite fait le lien : la belle-famille d'Ablyazov habite Genève, où elle emploie la moitié du barreau de la ville, et presque tous les détectives ! C'était signé. »

La cigarette d'après-rendez-vous est agitée : l'un d'entre nous pense que ce Rajat n'existe pas, que c'est un écran de fumée lancé par notre interlocuteur pour détourner l'attention de ses propres responsabilités. L'autre voudrait au moins tester la piste, potentiellement prometteuse.

Dans l'avion du retour, nous ruminons nos hypothèses à coups de « et si ? » et « souviens-toi… ». Cette irritante sensation de flou, ce sentiment permanent d'étreindre des ombres, ne vont plus nous quitter pendant toute la durée de notre enquête. Pendant des mois, nous allons enchaîner les épiphanies et les découragements, tout reprendre à zéro et nous disputer sur des détails. Bref, la route sera longue.

*

Paris, décembre 2016. Détenu en France depuis plus de trois ans, Mukhtar Ablyazov attend la décision du Conseil d'État, la dernière instance capable d'empêcher son extradition vers l'Ukraine ou la Russie. Le 9 décembre, elle tombe : alors que tous les tribunaux français et le gouvernement lui-même, ont validé l'expulsion de l'oligarque du territoire, les hauts fonctionnaires du Palais-Royal, eux, la refusent, arguant qu'elle a été « demandée pour un motif politique ». Les autorités kazakhes, expliquent-ils en substance, ont mené d'étroites « concertations » avec toutes les parties en présence pour arriver à leurs fins.

Les manœuvres auxquelles le Conseil d'État fait référence sont avant tout les opérations d'influence exposées dans les mails publiés sur Kazaword : les avocats de l'oligarque les ont joints à la procédure et leur contenu a visiblement fait son effet sur l'institution française, qui n'a annulé des décisions d'extradition qu'à deux reprises au cours de son histoire.

Le soir même, Mukhtar Ablyazov est libre. Mais l'opération de cyber-guérilla diplomatique a laissé des traces : sans attendre la libération de sa bête noire, le Kazakhstan a lancé une vaste offensive judiciaire contre le site Kazaword afin de faire disparaître toute trace des mails piratés. Et dans ses nombreuses plaintes, déposées aux États-Unis et en Nouvelle-Zélande, où est hébergé Kazaword, Astana accuse clairement le camp Ablyazov et sa belle-famille d'avoir orchestré l'opération de hacking. Les avocats du Kazakhstan insistent en particulier sur le rôle qu'aurait joué Muratbek Ketebaev, un ancien collaborateur de Mukhtar Ablyazov réfugié en Pologne. Son site, Respublika-kz.info, est le tout premier à avoir relayé les e-mails piratés. Ces assertions ne seront jamais contestées par l'intéressé ni par Mukhtar Ablyazov.

*

Paris, mars 2017. Faute de certitude sur l'identité des hackers israéliens, nous sommes toujours sur la piste de « Rajat », le mystérieux pirate qui a œuvré dans la guerre électronique entre le Kazakhstan et ses opposants. Non loin du Palais-Royal, nous retrouvons un enquêteur privé de haut vol, spécialiste des batailles boursières à plusieurs milliards d'euros. Nous le connaissons depuis dix ans, apprécions sa franchise et surtout son absence de sérieux : l'homme est capable de raconter les dessous sanglants d'une OPA comme s'il s'agissait d'un match de rugby entre vieux camarades… En outre, il a un goût prononcé pour les opérations « non conventionnelles », aux marges de la légalité : les meilleures… Nous sommes sûrs qu'il connaît certains des personnages que nous essayons d'identifier.

Devant des rognons de veau, nous parlons de choses et d'autres, jusqu'à, négligemment, lâcher le nom de « Rajat », « un hacker indien » dont nous « avons entendu parler ». La métamorphose est immédiate : notre interlocuteur se fige, pose ses deux mains sur la table et recule de quelques

centimètres : « Vous voulez me piéger, c’est ça ? » L’homme est métamorphosé : tendu comme un arc, il est livide et ne lâche plus que des phrases laconiques, les dents serrées. Gênés, nous comprenons que nous avons frappé trop fort et surtout trop près du but : notre invité, de toute évidence, connais très bien le mystérieux « Rajat » et l’a vraisemblablement fait travailler. Méfiant, il est persuadé que nous savions tout cela à l’avance, alors que c’est son attitude qui vient de nous le révéler ! En quelques secondes, l’atmosphère est à couper au couteau et, à notre grand dam, aucune serveuse ne vient détourner l’attention…

Nous faisons dériver la conversation vers des sujets plus terre à terre : comment pirate-t-on une boîte mail ? « Je comprends que ce n’est pas très difficile, explique notre interlocuteur, toujours sur ses gardes. Le vrai travail n’est pas vraiment informatique, mais social : il faut arriver à convaincre le propriétaire de la messagerie de cliquer sur un lien qui introduira dans son système un logiciel malveillant, dit “cheval de Troie”. C’est cette technique, appelée *phishing*, qui permet, en créant un accès, l’intrusion et le vol de messages. Sauf que tout cela ne peut marcher qu’avec la coopération involontaire de la cible. Il faut donc lui expédier un e-mail vraisemblable, émanant d’une adresse connue ou supposée telle, et dans laquelle le cheval de Troie est déguisé en pièce jointe inoffensive. » C’est ainsi qu’a été piégé John Podesta, le directeur de campagne de Hillary Clinton, dans une affaire dont nous reparlerons : il a cliqué sur un message émanant en apparence de Google et qui lui demandait de reconfigurer son mot de passe, apparemment compromis. Podesta a obtempéré et, en octobre 2016, tous ses messages ont été publiés par WikiLeaks.

« Pour connaître les habitudes de la cible, continue notre initié, les pirates étudient ses goûts sur les réseaux sociaux, son histoire personnelle, etc. La cupidité est un bon moteur : peu de gens résistent à ouvrir un courrier de leur banque. Mais la vanité marche aussi très bien : je connais plusieurs personnages importants, membres de conseils d’administration prestigieux, qui n’ont pu se retenir d’ouvrir un courrier les avertissant que leur page Wikipédia avait été modifiée… »

Nous aurons la confirmation de l’efficacité de ces méthodes lorsque nous rencontrerons, début avril, l’un des Français qui ont vu leurs mails exposés par Kazaword. Persuadés qu’il sait comment les pirates ont procédé, voire

qu’il dispose d’informations supplémentaires sur l’opération, nous aurons la surprise de l’entendre spéculer sur le *modus operandi* de ses assaillants… Durant l’entrevue, nous nous contentons de prendre des notes distraites sur des cahiers où s’étalent, à chaque page, des schémas de pénétration et les noms de hackers qui, potentiellement, pourraient avoir piraté sa messagerie…

*

À force de multiplier les entretiens, nous commençons à comprendre que le monde de la fuite massive est un univers perpétuellement mouvant, où les victimes sont toutes des assaillants en puissance. Une vérité qui se vérifiera sans cesse au cours de notre enquête.

Dans le dossier kazakh, le gouvernement d’Astana paraît la victime : ce sont les messageries de ses diplomates et de ses consultants qui ont été exposées sur Internet. Sauf que le Kazakhstan lui-même est soupçonné d’avoir mené des opérations de hacking ! Depuis 2013, le ministère public suisse enquête sur des tentatives de piratage dans trois études d’avocats genevoises : Schellenberg Wittmer, Lalive et Chabrier. Les trois cabinets ont un point commun : ils défendent tous les trois la belle-famille de Mukhtar Ablyazov, à savoir le clan Khrapunov, installé en Suisse. À deux reprises, les avocats ont été ciblés par des rafales d’e-mails piégés aux intitulés trompeurs : des prises de contact de potentiels clients, des rappels administratifs ou des incitations à télécharger… des logiciels anti-piratage !

Dans les plaintes qu’ils ont déposées auprès des autorités suisses, les ténors du barreau genevois ne font pas mystère de leurs soupçons : pour eux, l’opération a été montée par le Kazakhstan et par son sous-traitant favori, l’américain Arcanum Global Intelligence. Autrement dit, l’employeur de l’ancien directeur du renseignement intérieur français, Bernard Squarcini…

Ces accusations croisées seront une constante tout au long de notre enquête : dès qu’un interlocuteur se dira victime de piratage, nous ne tarderons pas à découvrir qu’il a pu lui-même commanditer des opérations similaires. L’univers du « Leak » ignore la morale : rien n’y est droit, et tout le monde ment.

Loin des images de cyber-soldats opérant dans des salles sécurisées, le monde du trafic de données est aussi profondément mercenaire : à tout moment, les hackers peuvent retourner leur veste et se mettre à travailler pour l'autre camp. En enquêtant sur le mystérieux « Rajat » dont nous ignorons toujours l'identité, nous avons compris qu'il était très connu dans le petit monde de l'enquête privée, même si la seule mention de son patronyme abrégeait les conversations. Mieux : en recoupant les informations fournies par nos différents interlocuteurs, nous avons acquis la certitude que le pirate indien avait activement travaillé pour des cabinets eux-mêmes employés par le Kazakhstan. Avant de changer de camp ? Les intrigues diplomatiques font figure de jeu d'enfant aux côtés des retournements d'alliance entre hackers…

À cet écran de fumée perpétuel vient s'ajouter un autre obstacle, plus structurel celui-ci : reconstituer une chaîne de responsabilités dans une attaque informatique est une tâche aussi hasardeuse qu'herculéenne. Dans son article « Attributing Cyber Attacks », publié en 2015 dans le très sérieux *Journal of Strategic Studies*, l'universitaire anglais Thomas Rid exclut toute certitude en la matière : les enquêteurs informatiques, explique-t-il, peuvent constituer un faisceau de présomptions en examinant le code-source des chevaux de Troie, et les sites-relais utilisés pour siphonner les mails. Mais une pénétration ne laisse généralement que peu de traces, et jamais la dissection d'outils informatiques ne permet de remonter jusqu'à un individu. Aurons-nous plus de chance avec nos carnets et nos stylos ?

Après des semaines à avancer en crabe, de source en source et de mensonge en demi-vérité, le découragement commence à poindre : la piste humaine est-elle la bonne ? En partance pour New York afin de rencontrer des hauts responsables américains, nous nous retrouvons dans une salle d'embarquement à Charles-de-Gaulle. L'un de nous arbore un sourire jusqu'aux oreilles : « J'ai tout. C'est énorme. Je te raconte dans l'avion. » Les remarques assassines fusent : c'est de la torture ! Deux bières, une bouderie et une démonstration de gilet de sauvetage plus tard, la réponse arrive enfin, sous la forme de notes griffonnées à la va-vite. « C'est ça, tout ? – Lis bien : j'ai retrouvé la trace d'un entrepreneur en "sécurité informatique" indien nommé Rajat Khare ! Des enquêteurs informatiques norvégiens lui auraient consacré une très longue étude, montrant qu'il mène

des piratages de messageries pour le compte d'une multitude de clients privés. » Si nous parvenons à mettre la main sur ce document, nous aurons définitivement identifié l'insaisissable « Rajat »… Mais est-ce bien lui qui a opéré dans la « guerre des fuites » kazakhe ? Et si oui, pour le compte de qui : le Kazakhstan ? Les oligarques en rupture de ban avec le régime ? Les deux à la fois ?

« Bien sûr que nous connaissons les auteurs du hack contre Bernard et le Kazakhstan ! Croyez-moi, ces types ne perdent rien pour attendre. » Nous sommes de retour à Londres, dans les spectaculaires locaux d'un fonds d'investissement qui travaille en lien étroit avec le Kazakhstan. Dans les bureaux spacieux qui dominent Green Park, des secrétaires sculpturales, juchées sur des talons d'au moins dix centimètres, slaloment entre les œuvres contemporaines et les meubles design. Avec nos sacs à dos et nos jeans, nous faisons un peu tache dans ce décor luxueux.

On nous fait entrer dans la *conference room* où nous rejoint le maître des lieux, dont le visage s'affiche sur tous les murs en compagnie des grands de ce monde : chefs d'État, hommes d'affaires, mais également champions de polo. Sans surprise, il refuse qu'on le cite, ni même que son nom n'apparaisse : « La discrétion est au cœur de mon métier, et le dossier qui vous occupe est ultra-sensible. » Nous commençons à en avoir l'habitude et parlons de choses et d'autres pour le mettre en confiance.

Au bout d'une heure de considérations géopolitiques, la discussion s'anime : les dirigeants du Kazakhstan, qui refusent obstinément d'évoquer la cyberguérilla qui les oppose à Ablyazov, ont apparemment une idée assez précise de l'identité des pirates qui les ont ciblés. Une fois encore, nous mettons le pied dans la porte : qui ? « Des Israéliens. Plus précisément d'anciens fonctionnaires du ministère de la Défense. » Nous sommes déjà sur cette piste, mais n'avons aucune certitude sur un nom. « Un ancien commando, reconverti dans la sécurité privée. » Cela, nous le savons, mais la description est encore trop vague : elle correspond à plus d'une cinquantaine de personnes ! « Nous avons des noms, mais nous devons vérifier auprès de notre client s'il est possible de vous les communiquer. Vous recevrez l'information par coursier spécial. Rentrez à Paris. Là-bas, un homme vous contactera et vous communiquera une lettre manuscrite. Sur ce courrier figureront les informations que vous cherchez. Vous disposerez de quelques minutes pour en prendre connaissance avant que le coursier ne

détruise le document. » Le scénario, tout droit sorti d'un film d'espionnage, était séduisant. Malheureusement, il ne s'est jamais produit. La fameuse lettre ne nous est jamais parvenue, et les noms sont restés des hypothèses.

Pourquoi ces irritantes valses-hésitations ? Les rodomontades de nos interlocuteurs ne sont-elles rien d'autre que du bluff ? Comment peuvent-ils se vanter de connaître les hackers ayant participé aux fuites kazakhes et, dans le même temps, refuser d'avancer le moindre nom ? À force de relancer chacun des acteurs et de recouper les miettes d'informations qu'ils veulent bien nous lâcher, l'évidence fini par s'imposer : si tous sont à la fois certains de leur fait et réticents à nous aider, c'est qu'ils ne peuvent nous donner aucun nom sans s'incriminer eux-mêmes ! Dans la guerre électronique qui a opposé le Kazakhstan à ses barons déchus, chaque camp a pratiqué le hacking à grande échelle en utilisant les mêmes prestataires. Identifier ces pirates, c'est tout à la fois accuser l'adversaire mais également exposer ses propres manœuvres… Le petit monde de la fuite massive est un univers particulièrement incestueux où tout le monde se connaît et se tient : les intrus dans notre genre ne sont pas les bienvenus.

Pour remonter jusqu'à la source des fuites kazakhes, il ne faut compter que sur nous-mêmes. Étant parvenus à identifier le fameux « Rajat » à partir de son seul prénom, nous tentons de faire de même avec ses collègues israéliens. Mais les indices sont maigres : nous savons qu'il s'agit de vétérans des bataillons de guerre électronique reconvertis dans le privé, et qu'ils ont pignon sur rue. Plusieurs centaines de personnes répondent à cette description… Un par un, nous passons en revue tout les suspect potentiels, écartant ceux dont l'expérience paraît trop réduite, l'activité trop légitime ou les talents insuffisamment diversifiés. Petit à petit, le cercle se réduit. Nous testons des noms auprès de nos « gorges profondes », oubliant ceux qui ne suscitent aucune réaction pour privilégier les patronymes qui abrègent les conversations. Au terme de ce travail de fourmi ne subsistent que quelques profils d'élite comme Israel Ziv, un vétéran des opérations clandestines reconverti dans la sécurité privée et la pénétration informatique ; Arik Gold, un cadre de la société israélienne d'interception téléphonique Ability, qui a compté parmi ses administrateurs l'ancien directeur du Mossad, Efraim Halevy ; et Tal Dilian, le fondateur de la petite

compagnie de renseignement électronique Circles, qui a dirigé le service des écoutes de l’armée israélienne.

Chacun de ces personnages a-t-il eu des contacts avec le gouvernement kazakh et ses ennemis ? C’est ce qui reste à déterminer. Pour cela, il n’y a d’autres solutions que d’aller voir de plus près.

II

Les cambrioleurs

Si les effractions électroniques et la publication des éléments piratés sont planifiées par des stratèges de la guerre électronique, les opérations de cybercambriolage sont assurées par des spécialistes. Il existe aujourd'hui un véritable marché mondial du hacking, où les pirates les plus habiles sont plus demandés que les footballeurs-stars. Dans ce mercato international, Israël et l'Inde dominent. Pour tous les professionnels de l'intrigue, c'est à Tel Aviv et à New Delhi que se recrutent les meilleurs artisans de la fuite massive. Ce n'est pas un hasard si tous les belligérants des cyber-batailles kazakhes sont venus puiser dans ces deux pays les compétences dont ils avaient besoin.

« Si vous voulez un hacking de précision, il vous faut un hacker israélien ! » Pourquoi cette phrase revient-elle si souvent dans la petite communauté internationale du renseignement privé ? Dans un univers pourtant peu porté sur la modestie, tout le monde s'incline devant les pirates du petit État hébreu.

Dans la fuite massive qui a visé le Kazakhstan, on trouve des opérateurs israéliens dans les deux camps, tant chez les oligarques en rupture de ban avec le régime que du côté du régime d'Astana. Selon plusieurs de nos sources à Washington et Tel Aviv, des consultants israéliens spécialisés dans la cyberguerre, tels Arik Gold de la société Ability Inc., ou des groupes comme Nice Systems ont mis le pied à Astana pour proposer leur savoir-faire aux services kazakhs de renseignement. Le nom de Tal Dilian a aussi émergé rapidement. Ce colonel a commandé de 1998 à 2002 l'unité 8100 du renseignement israélien, spécialisée dans les écoutes et le hacking de précision. Il a, plus tard, fondé la société Circles, devenue une référence du domaine, qui est aujourd'hui très bien connue des grands patrons de

l’espionnage kazakh. Ceux-ci ont tous voulu s’appuyer sur ces cyberespions israéliens pour cibler et infiltrer leurs adversaires dans le cyberespace. Pas étonnant que les adversaires d’Astana aient fait de même…

Un nom revient avec insistance lorsque l’on évoque les consultants spécialisés dans les cyber-opérations parallèles : celui d’Israel Ziv. Haut gradé de l’armée israélienne reconverti dans les opérations clandestines privées, il disposerait d’une équipe rompue aux techniques d’intrusion des réseaux. Mais l’ancien officier est loin d’être le seul à intervenir sur ce créneau : d’autres consultants, souvent issus des services de renseignement ou des unités militaires spécialisées dans les interceptions, ont également pignon sur rue à Tel Aviv.

Espions en service ou en retraite, diplomates de choc ou hommes d’affaires prospérant dans les pays sensibles : tous marquent un temps d’arrêt lorsqu’on prononce le nom d’Israël Ziv.

L’homme incarne à lui seul la professionnalisation de l’intrusion informatique en Israël. Et résume merveilleusement les ambiguïtés du secteur, entre opérations privées et commandes d’État. Cet ancien directeur des opérations de Tsahal, l’armée israélienne, s’est reconverti dans le secteur privé au début des années 2000, tout en restant très proche de l’establishment sécuritaire du pays. Il a alors fondé la société de sécurité Global CST, devenue aujourd’hui Global Group, avec Yossi Kuperwasser, qui fut à la tête du département « recherche » du renseignement militaire israélien (nommé Aman), et Amos Ben-Avraham, ancien commandant de la célèbre unité Sayeret Matkal, utilisée par l’armée et le renseignement israéliens pour leurs opérations clandestines en territoire ennemi. Global s’est très vite spécialisée dans la formation d’unités commandos à travers le monde, quitte à mener elle-même les opérations lorsqu’elles sont trop complexes ou trop délicates pour ses élèves. Dès sa création, Global a puisé dans le vivier des vétérans de l’armée israélienne, en particulier les jeunes retraités des forces spéciales, attirés par les salaires offerts par la société et les perspectives de missions d’envergure. En travaillant pour Ziv, ces hommes ont toujours considéré, à tort ou à raison, qu’ils continuaient à servir leur pays.

Loin de se limiter aux contrats de protection de puits de pétrole ou de mines de diamants dans des pays en guerre, la société d'Israel Ziv a également conclu des contrats plus sensibles, n'hésitant pas à se substituer aux services gouvernementaux dans plusieurs pays. L'ancien officier israélien s'est ainsi lancé, au début des années 2000, dans la formation des commandos d'intervention polonais, offrant à Varsovie de créer une version locale de la Sayeret Matkal. La Géorgie a également fait appel à lui pour réformer son appareil militaire.

Malgré les services très régaliens qu'il propose à ses clients, Israel Ziv se comporte avant tout en homme d'affaires : il répond à la demande et ne s'estime en aucun cas lié aux pays pour lesquels il travaille. Après la Géorgie, il n'a d'ailleurs pas hésité à proposer ses services à la république autonome d'Abkhazie, pourtant en conflit avec Tbilissi.

La seule fidélité de Ziv est envers Israël : il ne travaillera jamais contre les intérêts de l'État hébreu. Mieux : l'establishment sécuritaire israélien garde un droit de regard sur ses contrats. L'opération en Abkhazie a ainsi été bloquée *in extremis* par les diplomates de Tel Aviv, soucieux de ménager toutes les parties dans le conflit russo-géorgien. Surtout la partie russe…

Global a également été aperçue au Pérou et en Colombie, où la société devait former les troupes d'intervention du pays, notamment les commandos chargés d'infiltrer la guérilla communiste locale, les Forces armées révolutionnaires de Colombie (FARC). Ce sont ces soldats d'élite qui ont libéré la Franco-Colombienne Ingrid Betancourt, otage des FARC. Aujourd'hui, Global dispose de représentants au Soudan du Sud, le dernier-né des États africains, ravagé par une interminable guerre civile.

On retrouve également la trace d'Israel Ziv en Guinée, un des rares contrats où l'inamovible général s'est retrouvé en porte-à-faux, tant vis-à-vis de ses clients que des autorités israéliennes. Le capitaine Moussa Dadis Camara, arrivé à la tête de la Guinée à la faveur d'un putsch, a recruté Ziv pour former sa garde présidentielle. Mais, en septembre 2009, les élèves guinéens de ce dernier se sont rendus coupables d'un massacre, suscitant un scandale international et une enquête du ministère israélien des Affaires étrangères. Durant leur investigation, les diplomates ont réalisé que Ziv avait signé avec la Guinée avant même de recevoir l'imprimatur de Tel Aviv. Pour sa part, l'ancien officier reconverti a toujours maintenu qu'il avait obtenu l'autorisation du ministère israélien de la Défense, ce que des

sources proches de l'institution n'ont cessé de nier. La diplomatie israélienne a tout fait pour que l'appareil sécuritaire désavoue Israel Ziv, mais s'est heurtée à un mur. L'ancien ministre des Affaires étrangères social-démocrate Shlomo Ben-Ami, l'ancien ministre adjoint à la Défense Ephraim Sneh ou encore l'ancien ambassadeur d'Israël en France Nissim Zvili ont volé à la rescousse du général à la retraite, justifiant ses opérations.

Tout à la fois craint et respecté, haï par certains comme adulé par d'autres, Israel Ziv fait partie de ces personnages qui naviguent entre les univers gris de la sécurité privée et des intérêts d'État. Il a aujourd'hui considérablement réduit le nombre de ses voyages à l'étranger et demeure la plupart du temps en Israël, ce que d'aucuns interprètent comme une discrète mise à l'écart, un signe de désaveu de la part des services de renseignement du pays. Ses connexions au sommet de l'état-major israélien et son savoir-faire en matière d'opérations commandos en font cependant un personnage suivi à la loupe par tous les services de renseignement du monde. S'il venait à poser le pied dans un pays africain francophone, la DGSE se tiendrait immédiatement sur ses gardes.

Voir apparaître un personnage comme Israel Ziv dans le dossier du piratage et de la diffusion des e-mails du Kazakhstan nous a pris de court. Pour nous, il n'était qu'un professionnel des coups de force. Erreur… Les opérations de hacking ne sont que le prolongement dans le monde virtuel d'une longue tradition d'opérations secrètes à la frontière du privé et du régalien. Pas étonnant qu'elles soient pilotées *in fine* par les mêmes stratèges !

Dans la plus grande discrétion, le charismatique général a ainsi développé une petite activité de pénétration informatique. Plusieurs de nos sources lui attribuent d'ailleurs d'autres cyberopérations hautes en couleur, tout aussi impressionnantes qu'invérifiables. Peu versé dans la programmation, Ziv n'a pas constitué son équipe de hackers *ex nihilo*. En avril 2017, un autre ancien des forces spéciales israéliennes, attablé à nos côtés dans un délicieux restaurant de Washington, à quelques tables seulement du secrétaire d'État américain Rex Tillerson, nous révèle que Ziv a récupéré la colonne vertébrale et les principaux membres de l'ancienne

équipe de génies de l'informatique du *golden boy* israélien Oded David (O.D.) Kobo.

Ce serial-entrepreneur a fait fortune en fondant puis en revendant plusieurs start-up de jeux en ligne, toujours en partenariat avec des figures de la jet-set mondiale. On retrouve, parmi ses partenaires, des figures aussi connues que le géant libano-mexicain des télécoms Carlos Slim, l'oligarque russe Roman Abramovich, mais aussi des stars comme les chanteurs Will.I.Am, Nicki Minaj ou encore le DJ David Guetta. David Kobo a également investi aux côtés de fonds d'État, comme la Qatar Investment Authority (QIA). L'une de ses sociétés, Shellanoo, a notamment développé l'application de chat ultrasécurisé Blindspot, qui permet d'envoyer des messages anonymes. Celle-ci a été très critiquée pour sa capacité à faciliter les campagnes de harcèlement massif, notamment dans les lycées. L'ingénieur en chef de Blindspot n'est autre que Dor Rafaeli, le frère du top model israélien Bar Rafaeli, célèbre pour avoir été la compagne de l'acteur Leonardo DiCaprio.

Venu du monde gris de la programmation sauvage, Kobo n'a eu de cesse de vouloir normaliser son profil et de faire oublier ses débuts aventureux. À mesure qu'il alignait les succès et revendait ses sociétés, il s'est discrètement séparé des équipes de codeurs qui l'accompagnaient depuis le début. Ce sont certains de ces codeurs d'élite qui ont été récupérés par Ziv.

Familier de notre publication Intelligence Online, qui a souvent révélé ses opérations à travers le monde, Israel Ziv s'est d'abord montré intéressé par une rencontre lors d'un de nos passages à Tel Aviv. Puis il a pris le temps de réfléchir, longuement, et, apprenant que ses opérations militaires privées nous intéressaient moins que celles, plus secrètes, qu'il mène dans le cyberespace, il a finalement décliné. À notre grand regret : impossible de le confronter aux éléments qui tendent à impliquer ses équipes dans le piratage des boîtes mails du Kazakhstan et d'entendre ses explications, ou ses dénégations.

Mais Ziv n'est pas le seul Israélien à opérer dans les maquis du cyberespace. Et le hacking des messageries gouvernementales kazakhes est loin d'être le seul dossier où l'on retrouve des opérateurs basés à Tel Aviv. On ne compte plus les opérations de cyberrenseignement privé commandées par des consultants européens et américains à des sous-traitants informatiques israéliens. Pourquoi ce type d'opérations grises

prend-il son essor dans ce petit pays ? Comment cette bande de terre aride est-elle devenue l'un des terreaux les plus fertiles pour le piratage de précision ?

*

Mars 2017. Nous décidons de nous rendre directement en Israël pour trouver des réponses à nos questions. Notre voyage ressemble à un coup de poker : deux *goyim* s'intéressant aux arcanes des cyberopérations de l'État hébreu ne sont pas forcément les bienvenus dans la petite mais puissante communauté locale du renseignement.

Déambulant sous le soleil méditerranéen de ce début de printemps, entre les palmiers de la riviera de Tel Aviv et les ruelles escarpées de Jaffa, nous avons dû multiplier les canaux et montrer partout patte blanche. Nos écrits, nos interventions, ont été passés au peigne fin par tous les professionnels sollicités. Peu après notre arrivée, nous avons également eu la surprise de recevoir pendant une brève période nos SMS en double… Signe, selon l'un de nos guides, bien connecté dans le secteur, de l'intérêt que nous pouvons susciter à nos dépens.

L'un de nos premiers rendez-vous a donné le ton du séjour : devant l'entrée d'une bicoque anonyme dans la banlieue de Tel Aviv, nous avons été accueillis par un panneau proclamant : « *Violators will be shot, survivors will be shot again.* » Un bon test de notre motivation… Sans cesse, à chaque nouveau rendez-vous, il nous a fallu démontrer que notre démarche ne visait nullement à nuire à la sécurité de l'État hébreu, mais à comprendre les ressorts d'une nouvelle industrie qui s'épanouit aux marges des services régaliens et dont Israël est l'un des leaders incontestés. Par chance, certains de nos amis – grâces leur soient rendues ici –, très introduits dans l'establishment sécuritaire du pays, nous ont permis de nous faufiler dans le cœur du réacteur du cyberrenseignement israélien.

Une fois les obstacles levés et la méfiance (partiellement) dissipée, nous avons pu rencontrer, sur place, certains des opérateurs les plus inventifs en matière de « renseignement technique », le terme générique utilisé par les professionnels pour désigner toutes les opérations clandestines ciblant les flux des télécommunications. Le séjour fut mouvementé : sans cesse, il a fallu garder contenance, surveiller nos propos et tester les limites de nos

interlocuteurs. Tel Aviv est fondamentalement un village : tout le monde se connaît. Et dans ce village, le cyberrenseignement est un pâté de maisons. Plus qu'en France ou au Royaume-Uni, la petite communauté cyber israélienne fonctionne avec ses propres codes et s'organise autour de haines recuites et d'amitiés indéfectibles. Mille histoires d'opérations de haut vol, à peine croyables, y circulent, magnifiées par la faconde et les talents de conteurs de ceux qui les rapportent.

Sitôt arrivés, nous partons à la rencontre des principaux opérateurs privés de cyberrenseignement du pays, qu'ils soient spécialisés dans les interceptions ou les pénétrations informatiques. Malgré nos demandes, tous ont exigé de demeurer anonymes : difficile d'évoquer certains de ces contrats les plus sensibles à visage découvert. La plupart n'avaient d'ailleurs jamais rencontré de journalistes. Cette démarche n'était pour eux absolument pas naturelle, surtout dans un pays où l'armée peut toujours censurer certains articles dans la presse locale au nom de la sécurité nationale. Le fait d'être français a également suscité, au départ, la méfiance de certains de nos interlocuteurs : pour eux, la France est une nation pro-arabe, tant en politique extérieure qu'intérieure. Très en verve et charismatique à souhait, l'un d'eux se désespérait même que Paris soit devenu « Gaza-sur-Seine ». L'arak de Jaffa et le vin de Galilée ont finalement permis de balayer ces préventions.

Nous voulions comprendre pourquoi les opérations de piratage les plus audacieuses trouvaient leur source sûre dans ce petit pays. Entretien après entretien, nous sommes remontés jusqu'au l'origine du secteur cyberprivé israélien.

*

Lors d'un long déjeuner dans une petite trattoria nichée dans le quartier très branché de Neve Tsedek, à l'ombre d'une vigne grimpante, nous avons pu rencontrer quatre anciens officiers de Tsahal, tous professionnels du renseignement technique et aujourd'hui à la tête d'un des plus grands groupes israéliens de défense. Devant une myriade d'antipastis et la carafe d'un petit vin sec local qui semblait ne pas avoir de fond, ils nous ont raconté la genèse, presque légendaire, du cyberrenseignement israélien.

Au commencement était l'unité 8200, aussi appelée par les Américains Israeli National SIGINT Unit (INSU), dont au moins un de nos interlocuteurs était issu. Créée peu après l'avènement du pays en 1948, elle visait initialement à préparer l'armée israélienne au prochain champ de bataille : les ondes. Mais à mesure qu'Internet s'est développé, l'INSU s'est aussi intéressée au réseau mondial. Car, contrairement à d'autres pays, Israël s'est mobilisé très tôt pour investir le théâtre d'opérations virtuel : petit et entouré d'ennemis, il reste éternellement sur ses gardes et envisage toutes les éventualités pour ne pas être surpris. S'il ne veut pas tout simplement disparaître, l'État hébreu doit toujours frapper le premier. Dans cette optique, le renseignement est plus qu'un gadget : il est l'assurance de la survie.

Dédié aux interceptions et aux pénétrations informatiques, l'INSU est l'équivalent de la National Security Agency (NSA) américaine. Elle compte aujourd'hui plusieurs milliers d'agents, de programmateurs et d'ingénieurs. Ce sont ces bataillons électroniques qui, en collaboration avec leurs homologues américains, ont développé à la toute fin des années 2000 l'un des premiers virus informatiques à visée militaire, Stuxnet. Introduit dans les serveurs sécurisés iraniens en 2010, ce dernier a détruit une partie des centrifugeuses utilisées par Téhéran pour développer son programme nucléaire. De l'aveu même du directeur de la NSA de l'époque, Michael Hayden, la version finalement propagée dans les systèmes iraniens était beaucoup plus agressive que celle développée conjointement au départ.

Rencontré dans les jardins ombragés du Holon Institute of Technology, où il forme des étudiants à opérer sur un « cyber-champ de bataille » – une double rangée d'ordinateurs enfermés dans un laboratoire sécurisé –, un membre de l'équipe qui a travaillé sur Stuxnet se souvient de l'époque héroïque des cybercommandos israéliens : « Au début des années 1990, nous étions très impressionnés par la Chine, dont l'objectif était de dominer la sphère télécom en 2050. En infériorité stratégique face aux États-Unis, les Chinois avaient décidé d'investir tous leurs efforts dans le cyber, l'arme des pauvres. Évidemment, ce genre de raisonnement nous parlait au cœur… Nous avons donc rédigé une proposition pour l'état-major, dont la principale nouveauté était de supprimer la distinction entre attaquant et défenseur : dans le domaine cyber, ils doivent travailler ensemble. »

L’objectif des services de renseignement israéliens est alors de prendre le contrôle des infrastructures télécoms et les systèmes industriels, ceux-là mêmes que le virus Stuxnet mettra hors d’état de nuire en Iran. Mais, en trente ans, les pratiques ont changé et le nœud des cyberbatailles s’est déplacé vers les serveurs de messagerie et les téléphones portables.

Pour surveiller les réseaux de télécommunication, sa mission première, l’INSU doit en permanence développer de nouveaux outils et percer les cryptages les plus sophistiqués. L’une de nos sources à Paris nous mit sur la piste d’un « service dans le service » destiné à cette tâche, qu’il avait eu le privilège de visiter et dont nous avons pu, sur place, confirmer l’existence. Pour rester toujours à la pointe de la technologie, l’INSU dispose en effet d’un centre de recherche appelé par les initiés « The Farm » (la Ferme). L’existence de ce laboratoire interne, tenue soigneusement secrète, n’a jamais été révélée jusqu’ici. Et pour cause ! Les techniciens de ce département ultraconfidentiel ont notamment pour tâche de trouver des failles dans les dernières technologies de communication mises sur le marché, et notamment les applications sécurisées de messagerie mobile du type WhatsApp ou Telegram. Plus d’une centaine de chercheurs, tous issus des sciences fondamentales et de l’ingénierie, travaillent à la Ferme. Ils consacrent leurs journées à chercher de nouveaux algorithmes, de nouvelles manières de pénétrer les réseaux informatiques et de contourner les cryptages des meilleures applications. Ces chercheurs de la Ferme travaillent en étroite collaboration avec les opérateurs d’une autre cellule de l’armée israélienne, l’unité 8100, spécialisée dans les écoutes des télécommunications et les interceptions dites « tactiques », c’est-à-dire visant des individus. Les vétérans de ce laboratoire collaboratif de l’interception constituent un corps d’élite dans lequel piochent allègrement les entreprises privées.

Nous pouvons également révéler que, si l’INSU dispose d’un bataillon de pirates informatiques pour accompagner, voire préparer, les opérations militaires israéliennes, les hackers les plus offensifs dont dispose Israël se trouvent ailleurs, dans une unité ultrasecrète rattachée au Mossad, le célèbre service de renseignement israélien. L’un de nos compagnons de gueuleton, lui-même ancien du renseignement israélien, croisé dans un petit bar de plage de la marina de Tel Aviv, a brièvement évoqué ces cybercommandos

devant nous, avant de se raviser, par peur de mettre en péril la sécurité de son pays.

Cette unité du Mossad ne travaille pas, comme l'INSU, sur la pénétration massive des réseaux, mais sur des opérations beaucoup plus ciblées, le sur-mesure du hack. Ces tireurs d'élite du piratage se concentrent sur les réseaux d'un seul individu, ou d'une société soupçonnée de travailler contre les intérêts d'Israël. Ils sont sélectionnés dans les rangs de l'INSU, de l'unité 8100 ou d'autres services du Mossad, voire à l'extérieur des services israéliens. Si la cyberunité du Mossad peut travailler en collaboration sur certaines cibles, elle conserve son savoir-faire en interne et protège jalousement ses modes opératoires. Il nous a par ailleurs été confié à plusieurs reprises que, pour mener ses frappes dans le monde cyber, le Mossad entretient à l'extérieur de ses murs des équipes de hackers *freelance*, dont les motivations sont tout autant patriotiques que financières. Il n'est pas rare que ces chevau-légers travaillent, en parallèle, pour des intérêts privés, et notamment pour la myriade de sociétés développant des outils d'interception, des logiciels de sécurité informatique et toute une gamme de services de pointe pour le compte du renseignement israélien, mais également pour des gouvernements étrangers et des multinationales. Cette perméabilité entre le secteur privé et les services d'État est quasiment unique. C'est l'un des secrets de l'extraordinaire vitalité du hack « made in Israel ».

Parallèlement au développement de l'INSU, de l'unité 8100 et de son homologue du Mossad, s'est mis en place en Israël tout un écosystème de sociétés de cybersécurité privées. Le gouvernement de Tel Aviv aime à présenter le pays comme une « nation start-up », préfèrant néanmoins en avant les inventeurs d'applications téléphoniques révolutionnaires et de services en ligne plutôt que le petit noyau d'entreprises développant des outils d'interception sur Internet et surveillant les forums de hackers pour le compte des plus grandes banques du monde. Ces opérateurs discrets constituent pourtant la face cachée du « cyber-Israël », et l'une des principales forces du pays : les responsables informatiques des plus grandes entreprises et les dirigeants de tous les grands services d'interception du monde entier viennent faire leur marché en Israël.

La majorité des entrepreneurs en cybersécurité de Tel Aviv travaillent indifféremment, et parfois simultanément, pour des États et pour des entreprises. Leur extraordinaire développement a été largement facilité par la structure de la société israélienne et aurait été impossible dans un autre pays. Les cybermercenaires profitent notamment d'un vivier d'informaticiens unique au monde : au même titre que les autres corps d'armée, l'INSU a la particularité d'accueillir un nombre important d'appelés du service militaire, hommes et femmes, ce qui lui permet de repérer rapidement les futurs petits génies de l'informatique. Pendant leur service, ceux-ci acquièrent – s'ils ne les ont pas déjà – toutes les compétences nécessaires pour mener des opérations de cyberguerre. Ils apprennent également le cyberbricolage.

Si elle est très bien dotée financièrement par l'État, proportionnellement à la taille du pays, l'INSU est en manque chronique de fonds, ce qui encourage la débrouillardise et l'autonomie. Ce corps d'appelés constitue sans doute la cyberarmée la plus jeune et la plus structurée au monde. Devenus opérationnels à la fin de leur service, ces jeunes gens viennent grossir les rangs des start-up civiles qui pullulent dans le pays. Mais une part notable d'entre eux, après plusieurs années passées à mener des actions clandestines sur Internet, gardent un goût prononcé pour le renseignement. Et fondent ou rejoignent des sociétés qui interviennent en sous-traitant des services étatiques, ou bien comme cyberlimiers œuvrant pour le compte d'entreprises.

La suite de cette chronique orale de l'histoire du renseignement technique nous a été transmise, le soir de Pourim, par quelques-uns des cyberespions les plus truculents qu'il nous a été donné de rencontrer.

Alors que la fête célébrant le sauvetage des juifs d'Iran battait son plein sur une belle terrasse ensoleillée de Tel Aviv surplombant la Méditerranée, ceux-là nous ont narré, avec force détails épiques, la manière dont le secteur privé s'est emparé du cyberrenseignement, à la fin des années 1980. Ce soir-là, nous avons dû nous pincer pour être sûrs que nous ne rêvions pas : les cyberinitiés qui, toute la soirée, ont rivalisé d'histoires d'infiltrations clandestines et de détails techniques connus d'une poignée de personnes au monde étaient vêtus, comme le veut la coutume, de déguisements bariolés…

Au début des années 1980, donc, des anciens des unités électroniques de l'armée israélienne ont créé les premières sociétés privées de cyberrenseignement. La première a été Comverse, qui appartient aujourd'hui à l'un des champions nationaux, Verint. En 1993, Gil Shwed, un autre ancien de l'unité 8200, met sur pied Checkpoint, un autre géant de l'interception sur Internet. À cette époque, l'INSU n'avait aucune politique en matière de propriété intellectuelle : à quoi bon faire signer des contrats à des fonctionnaires qui partent dans le privé puisque le service reste en contact étroit avec eux ? Les programmateurs de l'INSU partent donc avec les logiciels qu'ils ont développés pour le compte de l'État et intègrent ces briques technologiques aux produits vendus par leurs entreprises… Face à la multiplication des reconversions et aux problèmes de dissémination que posaient ces transferts, l'INSU a, au début des années 1990, mis en place des règles : si les anciens fonctionnaires ont été encouragés à fonder des sociétés spécialisées dans le cyberrenseignement après avoir quitté l'unité, c'est l'État qui reste propriétaire des brevets développés durant leur années de service. Les sociétés dont les fondateurs ou des employés sont issus de ses rangs sont aujourd'hui légion : Cellebrite, Wintego, NSO, Magen, etc.

Les institutions étatiques, d'une manière ou d'une autre, gardent un contrôle étroit sur leurs anciens employés passés dans le privé. Les licences de vente à l'exportation, sésames pour les sociétés israéliennes vite bridées par l'étroitesse du marché local, ne sont accordées qu'aux entrepreneurs restés loyaux envers leur ancien service. Ceux qui franchissent la ligne jaune ne restent pas en activité très longtemps : tout le monde se connaît dans le cybervillage de Tel Aviv, et les nouvelles y vont parfois plus vite que sur les réseaux sociaux.

Si les renégats sont rares, c'est aussi qu'un passage au sein des unités 8200 ou 8100 vaut tous les discours marketing : tous les groupes mondiaux rêvent de se faire protéger par d'anciens cybersoldats israéliens, et aucune entreprise israélienne ne veut prendre le risque de se priver de cette aura en prenant les services de sécurité locaux à revers. Ceux-ci n'ont qu'à décrocher leur téléphone pour appeler les clients d'une société jugée insuffisamment coopérative pour signer son arrêt de mort : personne ne voudra plus travailler avec une entreprise désavouée par les responsables sécuritaires israéliens.

La menace n’est pas le seul instrument dont dispose le renseignement israélien pour contrôler les activités de ses anciens fonctionnaires. Maniant habilement le bâton et la carotte, le service aide ses ingénieurs qui veulent se lancer dans le privé en leur confiant un contrat, voire en détachant certains de ses chercheurs au sein de la nouvelle entreprise, à condition que celle-ci ne développe que des outils destinés aux États. Le nouvel entrepreneur dispose ainsi d’une force de travail gratuite et ultra-qualifiée… puisqu’elle est constituée de ses anciens collègues !

Au côté des géants de l’interception, d’autres sociétés fondées par des anciens de l’INSU, comme Kela Israeli Intelligence ou Clearsky, se sont spécialisées dans la surveillance du Darknet, cet Internet discret, non référencé par les moteurs de recherche, où tout le monde navigue anonymement *via* des protocoles spécifiques. Le Darknet est utilisé pour tous les commerces illégaux : vente de drogue, de numéros de cartes de crédit, de mots de passe etc. Mais c’est également sur ce réseau Internet parallèle que les hackers communiquent le plus, c’est là que se commandent les piratages et que s’achètent les failles de sécurité des messageries électroniques et des systèmes informatiques. Tous les grands établissements financiers emploient des consultants pour surveiller cette zone de non-droit virtuelle, s’assurer que leurs informations internes (comptes bancaires, listing clients) n’y sont pas proposées à l’achat, voire pour récupérer les données qui auraient fuité avant qu’elles ne soient exposées au grand jour…

C’est donc un véritable travail d’infiltration que proposent aux banques et aux fonds d’investissement ces consultants israéliens hyperspécialisés. Car le Darknet est un univers hostile : la paranoïa y règne, comme nous avons pu le constater nous-mêmes après avoir tenté de maladroites incursions sur certains forums très fermés.

La plate-forme se présente comme une longue suite ininterrompue de fils de discussion, le plus souvent sur fond noir. Le lieu n’est pas sans rappeler certains forums, tels Reddit ou jeuxvideos.com, connus pour leurs conversations réservées aux seuls initiés et où tout – le meilleur comme le plus grivois – circule. Seuls les initiés s’y retrouvent. Le jargon ultra-codé qui y prospère rappelle les discussions cryptiques des plus grands classiques de l’espionnage, façon OSS 117.

De nombreuses sociétés de renseignement financier européennes et américaines nous ont raconté à plusieurs reprises comment elles passaient commande de hacks sur ce réseau, où tout se paye en bitcoin, une monnaie électronique cryptée. Le plus aisé, nous a glissé dans un clin d'œil l'un de ces professionnels, est de disposer d'un « employé maîtrisant le cyrillique », l'alphabet russe, pour opérer sur les forums de hackers, voire pour passer commande d'un piratage.

Chaperonnés par leurs anciens services, les vétérans de l'unité 8100 et de l'unité 8200 bénéficient également d'un accès privilégié aux capitaux pour se reconvertir dans le privé. Rencontré dans un de ces bars de plage qui donnent à Tel Aviv un faux air de Miami, un ami un peu journaliste, un peu hacker, nous a ainsi dressé un panorama de la cyberfinance israélienne. Tout le secteur est alimenté par des fonds d'investissement locaux et les bureaux israéliens des poids lourds de la finance californienne. Lors d'un passage à New York, au printemps 2017, un ancien ponte nous a longuement détaillé l'écosystème financier du cyberrenseignement. Reconverti dans l'intermédiation entre start-up israéliennes et gestionnaires de capitaux américains, notre interlocuteur nous a notamment expliqué que les financiers investissant dans l'interception réseau sont, comme lui, passés par l'armée ou les services de renseignement. « Ils n'ont pas les pudeurs de leurs homologues européens quand il s'agit de prendre des participations dans des entreprises développant des technologies d'intrusion », nous a-t-il expliqué avec un grand sourire. Effectivement : une société comme le Mer Group, qui assure les interceptions Internet et télécoms pour le compte de plusieurs pays africains, aurait fait fuir n'importe quel *business angel* européen, inquiet des répercussions d'un tel investissement sur son image. Mais, pour un fonds comme l'israélien FIMI, c'était la cible idéale : Mer ne dispose-t-elle pas d'une filiale, Athena GS3, dont le responsable n'est autre que… Shabtai Shavit, l'ancien directeur du Mossad ? FIMI est donc entré au capital de Mer. Même appétit pour la surveillance chez le Californien Francisco Partners, qui a racheté coup sur coup deux opérateurs de surveillance israéliens : le petit groupe NSO, spécialisé dans l'exploitation de failles informatiques, ainsi que Circles, tourné vers l'interception des communications cellulaires.

Les services d'État israéliens ont beau travailler en association étroite avec les entreprises de cybersurveillance, au point qu'il est parfois difficile de savoir qui est qui et qui fait quoi, cette proximité ne s'est jamais transformée en vulnérabilité. Aux États-Unis, plusieurs fuites massives de documents confidentiels sont imputables à des consultants privés détachés au sein des agences de renseignement : Edward Snowden, par exemple, officiait au sein de la National Security Agency, mais travaillait pour une société privée, le cabinet de conseil Booz Allen Hamilton. Grâce aux accès dont il bénéficiait comme consultant, il a subtilisé des téraoctets de documents confidentiels. Rien de tel en Israël, où les responsables sécuritaires ne semblent pas considérer que le recours au secteur privé constitue un risque, contrairement à leurs homologues européens, et tout particulièrement français, qui refusent toute coopération avec le secteur privé au nom de la protection du secret.

*

Pour opérer sur le Darknet, l'INSU dispose d'un avantage déterminant. Pendant leur période de service, les agents de ce service se dotent d'une identité virtuelle, appelée avatar, pour pénétrer les forums les plus fermés consacrés au piratage, aux échanges de données, etc. Ces alias sont d'abord des pseudonymes, mais également tout un ensemble de caractéristiques virtuelles : centres d'intérêt, habitudes de connexion, façon de parler, etc. Une fois établies, ces cybercouvertures sont mises en scène sur les réseaux ; sous avatar, les fonctionnaires de l'INSU établissent des liens avec les autres membres du forum, contribuent aux discussions… Dans le Darknet, rester passif vaut exclusion. Il faut agir, échanger, et surtout laisser des traces. Car il en est de cet Internet clandestin comme des bars louches : les nouvelles têtes ne sont pas bienvenues. Pour gagner accès aux forums les plus fermés, il faut s'être constitué pendant des années une épaisseur virtuelle et une réputation en ligne. Premiers à avoir investi ce créneau, nombre d'agents israéliens ont travaillé pendant des années à mettre en scène leur identité virtuelle, désormais indétectable, même pour les hackers les plus chevronnés. Ces cybercouvertures, et les vraies personnes qui les opèrent, valent aujourd'hui une fortune sur le marché. Or les services israéliens autorisent les agents qui se reconvertissent dans le privé à

conserver leur personnalité virtuelle. Un cadeau inestimable, et un avantage décisif sur la concurrence, car hors d'Israël, les agents ayant opéré sur les réseaux doivent abandonner les avatars développés durant leurs années de service quand ils cessent d'être fonctionnaires. Mieux : l'État hébreu, contrairement à la majorité des pays européens, n'interdit pas aux entreprises présentes sur ce marché d'opérer cachées sur Internet (et, *a fortiori*, sur le Darknet). Ailleurs – et tout particulièrement en France –, l'utilisation de fausses identités pour surveiller les réseaux est strictement réservée aux services d'État. En élargissant au secteur privé des pratiques habituellement limitées aux fonctionnaires habilités, Israël a conféré à ses entreprises une supériorité considérable et leur a permis de monopoliser en quelques années le marché mondial de la sécurité des réseaux bancaires et de télécommunication.

Sous un palmier luxuriant, notre ami mi-journaliste, mi-cyberbricolo, nous révèle qu'aujourd'hui il existe une forte pression américaine pour qu'Israël régule le secteur du cyberrenseignement. Washington veut que Tel Aviv se dote de procédures réglementaires pour contrôler les cyberarmes qui sont développées par le privé, notamment celles qui ont vocation à être vendues à l'étranger. Sauf que, côté israélien, on rechigne à encadrer le secteur. Et les plus réticents ne sont pas les services de renseignement ni les sociétés concernées, comme on pourrait s'y attendre, mais les fonds d'investissement qui ont pris des participations au capital des opérateurs israéliens de cyberrenseignement. Si la vente à l'export de services de cybersurveillance et d'interception devait se raréfier, c'est toute la valorisation économique du secteur qui s'effondrerait.

Enfin, le secteur du cyberrenseignement privé n'existerait pas en Israël si les hackers locaux ne disposaient pas d'une assurance quasi unique au monde : au cas où leurs activités dans des pays étrangers venaient à être découvertes ou, pire, si leurs noms apparaissaient dans une enquête judiciaire, ils sont quasiment certains de n'être jamais extradés dans un pays tiers, l'État hébreu ne livrant que très rarement ses ressortissants à des juridictions étrangères. Cela n'empêche pas certains opérateurs israéliens de se faire prendre la main dans le sac hors de leurs frontières. Ainsi, plusieurs employés d'une société de cyberenquête de Tel Aviv, Black Cube, se sont vu accuser d'avoir pénétré les e-mails de la procureure anticorruption de

Roumanie, Laura Codruta Kövesi, et ont été arrêtés et emprisonnés à Bucarest, fin 2016, alors qu'ils n'avaient pas encore eu le temps de quitter le pays. Les autorités roumaines ont par la suite bien tenté d'émettre un mandat d'arrêt européen pour entendre les dirigeants de la société, mais sans espoir de succès : il était certain que ceux-ci ne quitteraient alors pas Tel Aviv, protégés par la quasi-immunité juridique offerte par Israël à tous ses citoyens.

L'assurance de la non-extradition permet ainsi aux opérateurs privés de cyberrenseignement de pouvoir proposer des produits et des prestations beaucoup plus audacieuses et offensives que bien de leurs concurrents. Combien de fois avons-nous entendu, dès qu'un piratage s'avère un peu spectaculaire ou des interceptions sauvages particulièrement habiles, les victimes dépitées attribuer l'opération à des « Israéliens » anonymes ? Combien d'enquêtes informatiques mènent-elles à Tel Aviv avant de se perdre dans le maquis des PME ultraspécialisées, inconnues des non-initiés ? Combien de techniciens israéliens aux attributions vagues et au portefeuille garni de cartes de visite interchangeables croise-t-on dans les capitales les plus exotiques ?

Globalisé, le monde de la fuite massive ne se limite cependant pas à Israël. Dans la guerre virtuelle qui a opposé, entre 2014 et 2016, les oligarques en rupture de ban avec le régime kazakh, les fantassins venaient de Tel Aviv, mais également de New Delhi, autre capitale mondiale des cyber-opérations noires.

*

Rajat Khare a aujourd'hui tous les attributs du jeune prodige des start-up indiennes. Issu d'une des plus grandes familles de l'establishment indien, il a fondé plusieurs sociétés, publié des manuels sur la cybersécurité, et n'hésite pas à poser en compagnie du prince William d'Angleterre et de sa femme Kate lorsque le couple voyage dans l'ancien Empire des Indes. Rajat Khare a même reçu en avril 2016 un financement de l'United Kingdom Trade & Investment (UKTI), l'agence gouvernementale britannique qui soutient les investisseurs à l'étranger, pour fonder sa dernière société, baptisée aReputation et qui se propose de gérer l'image en ligne de

personnalités. En clair, de nettoyer dans les moteurs de recherche tous les liens qui ne plaisent pas à ses clients…

Véritable figure de la Silicon Valley locale, il est récemment entré au conseil d'administration du conglomérat Punj Lloyd, l'une des fiertés capitalistiques du pays. Très actif dans les services parapétroliers pour le compte des géants mondiaux de l'énergie et du pétrole, ainsi que dans la construction et les travaux publics, le consortium est présent dans toute l'Asie, au Moyen-Orient et en Afrique. Punj Lloyd se développe depuis plusieurs années dans la défense, en particulier dans les nouvelles technologies. À noter qu'un de nos hackers d'élite israélien, croisé plus haut dans notre histoire, Tal Dilian, est aussi devenu récemment administrateur de ce conglomérat. Coïncidence ?

Rajat Khare est même depuis 2014 le très officiel ambassadeur de bonne volonté du micro-archipel caribéen Antigua-et-Barbuda, qu'il conseille sur la promotion du tourisme, les investissements étrangers et… les solutions de sécurité intérieure, comme par exemple les interceptions des télécommunications.

Négligé par les Occidentaux pendant longtemps, le secteur du cyberrenseignement privé a explosé en Inde ces dernières années. Du fait d'une politique très incitative des pouvoirs publics et des services de renseignement locaux, un microcosme spécialisé dans les cyberopérations a rapidement émergé, au point de devenir aujourd'hui l'une des références du secteur, prisée même pour les opérations de haute volée entre oligarques.

Aiguillés par les confidences des principaux protagonistes de la fuite massive de données du Kazakhstan, nous avons mis plusieurs mois à retrouver la trace de Rajat Khare. Car l'homme cultive plusieurs visages, l'un public, très glamour, et un plus discret, sous lequel il mène des cyber-opérations clandestines.

Pour tous ceux qui le connaissent, l'homme fait figure de prince noir indien du hack. Contacté, il n'a pas donné suite à nos demandes de rencontre. Sans doute a-t-il vite noté, comme Israel Ziv avant lui, que ce n'étaient pas tant ses activités philanthropiques qui nous intéressaient que les opérations de hacking qu'il mène pour le compte des entreprises et des

États. Auteur d'un livre sur l'« ethical hacking », 344 pages consacrées aux moyens légaux d'assurer la cybersécurité des entreprises, Rajat Khare est en effet un produit chimiquement pur de l'écosystème du renseignement technique indien, à la frontière des intérêts d'État et d'activités plus lucratives.

L'homme est longtemps passé sous notre radar. Lorsque plusieurs interlocuteurs nous ont assuré que les mails de la diplomatie kazakhe et de Bernard Squarcini avaient été piratés par une équipe indienne, nous avons de prime abord eu du mal à y croire. Jusqu'à ce que nous retrouvions, au terme de plusieurs mois de recherche, la trace d'un mystérieux « Rajat », et que nous apprenions que ses activités clandestines avaient fait l'objet d'investigations en Norvège. Obtenir copie de cette enquête fut long : notre prince indien du hacking n'a jamais fait l'objet de la moindre procédure pénale, et s'il est connu comme le loup blanc dans le petit secteur de l'enquête privée, personne ne veut parler de lui, et encore moins lui nuire, tant il a su se rendre indispensable.

C'est l'obstination qui a fini par payer. À force de bombarder tout le monde de questions faussement innocentes sur « un certain Rajat », un consultant, pressé de faire cesser « l'interrogatoire », nous a tendu une serviette en papier avant de tourner les talons sans un mot. Inscrit au stylo-bille dans la cellulose, un nom, celui d'une obscure société américano-scandinave de cybersécurité, Norman Shark. Quel rapport avec notre « Rajat » ?

En 2013, Norman Shark a été mandaté par le géant des télécoms norvégien Telenor pour enquêter sur une campagne de hameçonnage par e-mail (*spear phishing*) qui avait ciblé la direction du groupe. Le résultat de ces investigations, un rapport d'une quarantaine de pages que nous avons pu nous procurer, attribue l'attaque qui a visé Telenor à un groupe de hackers indiens. Mieux : en analysant les structures de codes utilisées lors des tentatives de piratage ainsi que dans les liens qui ont servi à infecter les messageries du groupe norvégien, les informaticiens de Norman Shark ont retrouvé la trace d'une petite société d'informatique indienne, Appin Technologies. Or Appin est la société d'un certain… Rajat Khare ! Nous tenions enfin notre *condottiere* du hacking indien.

C’est toute une infrastructure, cachée dans les méandres du Web, qu’Appin a mise en place pour mener ses cyberattaques. Assistés du Norwegian Computer Emergency Response Team (NorCERT, l’autorité publique norvégienne de cybersécurité) et de la National Security Authority d’Oslo, l’équivalent de la NSA américaine, trois chercheurs de Norman Shark, Snorre Fagerland, Morten Kravkik et Jonathan Camp, ont travaillé pendant des mois. Et ce qu’ils ont découvert était, pour eux comme pour nous, inédit. En enquêtant sur l’intrusion dans les réseaux de Telenor, les trois techniciens ont récupéré des logiciels malveillants (*malwares*) utilisés lors de l’attaque, ainsi que des noms de domaines et des adresses IP – le numéro d’identification de chaque appareil et/ou utilisateur qui se connecte sur l’Internet –, mettant en évidence un réseau dans le réseau, entièrement dévolu à la cyberoffensive.

À partir de cette cartographie des schémas de l’attaque, et de leurs propres archives, les cyberenquêteurs ont patiemment remonté la trace des assaillants. Fastidieux travail de fourmi, qui a, pour une fois, payé ! En suivant notamment la trace d’un des virus confectionnés par le groupe, sobrement baptisé HangOver, Norman Shark est remonté jusqu’à de nombreuses opérations de piratage, menées par l’équipe de Rajat Khare pour des entreprises ainsi que pour l’État indien.

Qui étaient les commanditaires de ces piratages ? Les enquêteurs de Norman Shark ne l’expliquent pas, mais, à la lecture de leurs travaux, nous sommes en mesure de combler les blancs. Car nous connaissons bien les incidents qu’ils dissèquent : chacun des piratages menés par l’équipe de Rajat Khare est lié à une bataille financière de haut vol sur laquelle nous avons régulièrement écrit durant ces cinq dernières années dans notre lettre d’information Intelligence Online. À la description faite par le rapport, il ne fait aucun doute que les intrusions informatiques menées par Rajat Khare et son équipe participent de ces guerres de conseils d’administration, qui se sont soldées, pour certains, par des fuites massives de données sur Internet ou dans la presse…

Ainsi, le rapport ne le mentionne pas, mais si Telenor mandate Norman Shark début 2013 pour enquêter sur les attaques informatiques qui ont visé ses cadres, c’est que le groupe norvégien, à cet instant précis, sort tout juste d’une bataille commerciale avec le conglomérat russe Alfa de l’oligarque Mikhaïl Friedman. Disputant à Telenor le contrôle du réseau cellulaire

ukrainien Vimpelcom, ce dernier avait jeté toutes ses forces dans cette bataille dont l'enjeu se mesurait en dizaines de millions de dollars. Pour faire plier Telenor, il avait mandaté les enquêteurs privés les plus agressifs du secteur. Certains d'entre eux ont-ils fait appel à Rajat Khare pour pénétrer les réseaux de Telenor ? C'est l'hypothèse qu'énonce, preuve à l'appui, le rapport de Norman Shark.

Grâce aux informations compilées dans ce document, nous nous sommes aperçus que les hackers de Rajat Khare avaient, en plus de Telenor, pénétré d'autres réseaux de sociétés elles aussi engagées dans de dantesques guerres capitalistiques ! Le plus emblématique est sans conteste le piratage des réseaux du groupe géant minier Bumi PLC.

En 2012-2013, ce conglomérat indonésien a été l'objet d'une guerre d'une violence inouïe entre ses deux principaux actionnaires, la dynastie d'affaires indonésienne Bakrie et le financier Nathaniel Rothschild, descendant de la branche britannique de la célèbre famille de banquiers. À l'instar de l'oligarque Mikhaïl Friedman, Nat Rothschild ne recule devant rien pour faire prévaloir ses intérêts et recourt également beaucoup aux prestigieux cabinets d'enquête de la place de Londres. Le conflit entre lui et le clan Bakrie, chacun détenant environ un tiers du capital de Bumi, s'est terminé devant la Cour de justice de Londres. Or, dans ce procès, un mystérieux lanceur d'alerte a fait parvenir aux avocats de Rothschild des documents échangés électroniquement au sein du conseil d'administration de Bumi entre les membres de la famille Bakrie. Ce lanceur d'alerte n'était autre que les hackers de Khare, qui ont fourni aux avocats de Nathaniel Rothschild toute la « documentation » nécessaire pour nourrir leur dossier contre la famille Bakrie. Il s'agit, on le voit, d'un *modus operandi* bien rodé.

Une autre cible des cybermercenaires de Rajat Kahre fut le conglomérat minier anglo-kazakh Eurasian Natural Resources Corporation (ENRC, aujourd'hui Eurasian Resources Group), contrôlé par les oligarques Alexander Mashkevitch, Patokh Chodiev et Alijan Ibragimov. Au printemps 2013, les trois actionnaires se disputent, plongeant leur groupe ENRC dans la tourmente. Chacun mandate ses propres enquêteurs pour taper sur les autres.

Selon nos informations, au moins l'un des cabinets engagés dans la bataille a également travaillé pour Nat Rothschild, donc potentiellement

employé le groupe de Khare. Et, de fait, les hackers indiens vont rapidement intervenir dans la guerre des chefs kazakhs qui déchire ENRC. Comme par enchantement, plusieurs administrateurs de la société reçoivent des courriers contenant des virus ou des liens vers des sites d'hameçonnage. Novices en informatique, ces vétérans de la City ne se méfient pas et cliquent : leurs messageries sont immédiatement aspirées… Certains des e-mails piratés seront envoyés anonymement à des quotidiens britanniques qui, faute de pouvoir établir avec certitude leur provenance, ne les publieront pas.

Les équipes de Khare ont même réussi l'exploit d'infiltrer l'une des plus grandes Bourses du monde, le Chicago Mercantile Exchange (CME). Utilisant une adresse électronique presque similaire à celle des salariés de la place de marché (cmegroups.net au lieu de cmegroup.com), ils sollicitaient, au nom des autorités boursières, des informations confidentielles auprès des sociétés cotées. Pour les revendre à des investisseurs en quête de « tuyaux » infaillibles ? Le recours aux pirates est de plus en plus répandu chez les courtiers en Bourse : en mars 2016, le financier français Dominique Romano a dû s'acquitter d'une amende de 7,92 millions de dollars auprès de la SEC, le gendarme de la Bourse américaine. Son crime ? Avoir reçu, quelques heures avant leur publication, les résultats financiers de grandes entreprises cotées telles Boeing, Caterpillar, DuPont, HP, Ford, etc. Ces données étaient piratées par des hackers ukrainiens sur les serveurs de plusieurs agences de presse financière comme Business Wire, PR Newswire et Marketwired.

Parallèlement à toutes ces guérillas commerciales, les équipes de Rajat Khare ont également, et parfois simultanément, opéré pour l'État indien, en particulier pour le Research & Analysis Wing (R&AW), le puissant service de renseignement extérieur du pays. Appin a ainsi mené de véritables *cyber-black operations* contre les ennemis de New Delhi, aux premiers rangs desquels le Pakistan, mais également les intérêts publics chinois, en particulier militaires. Plus étonnant, le groupe de hackers a cherché et parfois réussi à pirater les serveurs et adresses e-mails du mouvement du Khalistan, un groupe indépendantiste qui veut établir un pays sikh souverain dans la région du Pendjab indien. Mêmes tentatives de pénétration dans les serveurs du mouvement du Nagaland (ou Nagalim), un

groupe sécessionniste de l’ethnie naga, dans le Nord-Est de l’Inde. Deux objectifs qui laissent deviner une implication directe des autorités de New Delhi : aucun groupe privé n’aurait un intérêt particulier à pénétrer les serveurs de ces groupuscules minoritaires et violemment opposés à l’État indien.

*

Comment Rajat Khare, ce fils de bonne famille, a-t-il pu devenir une telle légende du hack ? Son environnement familial, à lui seul, constituait déjà un terreau favorable. Selon plusieurs de nos sources, l’oncle du cyberentrepreneur serait l’ancien patron de la police de Bombay, tandis que son beau-père aurait dirigé le R&AW, le tout-puissant service de renseignement extérieur indien, en charge de la surveillance du Pakistan, des réseaux djihadistes dans le pays, ainsi que de la Chine.

Rajat Khare a fondé Appin avec son frère Anuj. Officiellement, la société est uniquement active dans la cybersécurité, pour le compte de sociétés informatiques (Microsoft India), industrielles (Huawei, Daikin) et médiatiques (IndiaTimes, India Today). Elle sécurise également les réseaux de plusieurs institutions publiques, notamment des gouvernements locaux, des ministères et même le National Informatics Centre ! Mais nous avons pu nous procurer un document ultraconfidentiel qui montre que Rajat Khare n’est pas seulement un prestataire de services informatiques comme on en trouve des milliers en Inde. En 2011, le gouvernement indien a lancé un appel d’offres pour doter la police nationale d’un système d’interception des données informatiques et de surveillance de l’Internet ; sur la liste des sociétés retenues pour ce méga-contrat de surveillance figure… Appin Software Security ! Non content d’opérer clandestinement pour le compte des services indiens, le groupe de Rajat Khare est donc un fournisseur officiel des autorités indiennes.

En plus d’Appin, Rajat Khare contrôle plusieurs autres compagnies. Il a fondé, on l’a vu, un cabinet de nettoyage de référence sur Internet, aReputation, qui reçoit le soutien du gouvernement britannique. Il s’est également investi, avec son frère, dans une nouvelle société, Prophecis Technology, basée dans l’État de l’Uttar Pradesh. À la frontière de

l’intelligence artificielle et de la finance, celle-ci cherche, grâce à de puissants algorithmes, à anticiper les tendances des marchés boursiers, afin d’optimiser ses gains. Une alternative légale à l’hameçonnage d’informations de marché mené par Appin sur le Chicago Mercantile Exchange…

Comme en Israël, le secteur du cyberrenseignement indien, dont Rajat Khare est l’une des figures les plus en vue, n’est pas apparu par hasard. Il est la conséquence directe d’une politique publique destinée à combler le retard de l’Inde en matière de renseignement. New Delhi a misé sur le cyber parce qu’il s’agit de l’arme la plus rapide et la moins coûteuse à développer. Une fois ce choix stratégique effectué, le pays s’est appliqué à développer un véritable écosystème du cyberrenseignement.

Pour atteindre leur objectif, les autorités indiennes ont d’abord travaillé à mettre sur pied une jeune cybergarde prétorienne *via* l’Indian Institute of Technology (IIT) de la capitale, une école couvée par les services locaux de renseignement et offrant les formations les plus complètes de tout le sous-continent. Presque tous les ingénieurs des sociétés de cyberrenseignement indiennes sont passés par cet institut, où a également été formé Rajat Khare. Le cybercorsaire a gardé des liens avec son ancienne école puisque sa société, Appin, dispose de son propre laboratoire dans l’IIT.

L’institut sert en outre de pépinière aux agences de cyberrenseignement indiennes, au premier desquelles la National Technical Research Organisation (NTRO), l’agence d’interception indienne, l’équivalent local de la NSA américaine et de l’unité 8200 israélienne. À l’instar de ses homologues étrangers, la NTRO cherche actuellement à améliorer ses capacités en matière de pénétration réseau et a récemment mis en place un centre de recherche ultrasecret, le National Institute of Cryptology Research and Development (NICRD), qui teste chaque jour de nouveaux moyens pour pénétrer les réseaux de télécommunication et les applications sécurisées.

Comme en Israël, les agents du NTRO ne restent dans ces services que quelques années avant d’aller faire fructifier dans le privé les compétences acquises dans le public. Certains rejoignent les légions de sociétés de cybersécurité qui fleurissent dans le pays. D’autres veulent au contraire conserver un pied dans le monde gris de l’espionnage, tant par goût du

risque que par appât du gain : les contrats d'opérations clandestines sur Internet sont en effet bien plus rémunérateurs que les banals audits de sécurité. Ces agents, à l'instar de Rajat Khare, gardent alors un lien fort avec leur ancienne « maison », la communauté indienne du renseignement, et offrent des services « spécialisés » aux entreprises engagées dans des bras de fer violents avec leurs concurrents.

Selon plusieurs de nos interlocuteurs, les autorités indiennes, qui veulent favoriser la constitution de grands groupes indiens de cyberrenseignement, laissent de très vastes marges de manœuvre aux sociétés qui veulent se lancer dans les cyberopérations clandestines. Parallèlement à leurs activités commerciales, celles-ci peuvent en effet rendre de menus services, si nécessaire… Et les hackers indiens sont très populaires chez les sociétés de renseignement privées, américaines ou britanniques.

Comme en Israël, l'émergence de hackers chevronnés résulte d'un choix politique, celui de ne pas concentrer la totalité des moyens cyberoffensifs de l'État uniquement à l'intérieur de ses services et d'avoir en permanence à disposition des acteurs privés discrets, qui peuvent, le cas échéant, servir de fusibles…

C'est la voie choisie par un autre pays, la Russie, qui a aussi développé très tôt le recrutement de *freelances*. Patrie des meilleurs joueurs d'échecs du monde, Moscou a compris avant tout le monde que ses intérêts stratégiques pouvaient être efficacement défendus ou poussés par des fuites massives de documents, perpétrées contre ses adversaires par des pirates sous contrôle.

III

Les stratèges

À force d’être victimes de fuites massives de données, certains États se sont eux-mêmes saisis de cette pratique dont ils ont douloureusement expérimenté les ravages. Quelle meilleure arme que d’exposer les turpitudes d’un adversaire militaire ou d’un rival géopolitique en divulguant publiquement tous ses secrets ?

La Russie est sans doute le premier pays à avoir compris que la fuite massive de données n’était pas seulement une menace, mais également une opportunité. Rien d’étonnant à cela, comme nous l’a confié, dans le coin d’une discrète salle de restaurant de Washington, un ancien haut fonctionnaire du renseignement militaire russe : « Depuis la guerre froide, le KGB devenu le SVR forme ses recrues dans trois spécialités : l’analyse, la collecte d’informations, mais aussi la manipulation. C’est l’un des seuls services de renseignement du monde où la propagande et la contre-propagande sont considérées comme une discipline noble, et non comme une activité dégradante. » Professionnels de la manipulation, les services de sécurité russes disposent également d’une longue expérience en matière de chantage. L’une de leurs techniques favorites est le *kompromat*, qui consiste à accumuler des éléments compromettants (vidéo en galante compagnie, preuves de corruption, etc.) contre une cible et à les publier au moment opportun… Forte de ces traditions, la Russie, à l’inverse de ses homologues occidentaux, a tout de suite perçu le potentiel que constituaient les fuites massives, et a très tôt élaboré un *modus operandi* pour se saisir du procédé. Le professeur en études de sécurité du King’s College, Thomas Rid, qualifie le mode opératoire russe de « *hacking-and-leaking operations* » (HLO). La Russie est sans doute le premier État à avoir élevé la fuite massive de données au rang d’art politique, et à en avoir fait un instrument

supplémentaire dans son arsenal déjà très complet de techniques d’espionnage et d’influence.

22 juillet 2016. En pleine campagne présidentielle américaine, la plate-forme de diffusion de fuites massive WikiLeaks publie des milliers de documents internes au Comité national démocrate, l’organe dirigeant du Parti démocrate américain, celui de la candidate Hillary Clinton. Les chaînes américaines de télévision enchaînent les directs, et Washington entre en ébullition. Rebelote en octobre 2016, quelques semaines seulement avant le jour de l’élection, prévue le 8 novembre. Les mails piratés révèlent notamment un haut degré de collusion entre Hillary Clinton et le Comité national de son parti, et ce, au détriment de son challenger à la primaire, le radical Bernie Sanders. Hormis quelques pépites, peu d’informations apparaissent véritablement gênantes : cette fuite organisée vise davantage à déstabiliser la campagne électorale de la candidate démocrate qu’à susciter un réel scandale. « En sortant de nouvelles informations tous les jours, WikiLeaks prouve qu’il n’est qu’un bras armé pour la propagande du Kremlin, faisant le sale travail de Vladimir Poutine pour aider à faire élire Donald Trump », réagira dans la foulée de la dernière fuite d’octobre le porte-parole de Hillary Clinton. Car contrairement à la candidate démocrate, qui n’a cessé de dénoncer l’ingérence russe en Ukraine et en Syrie lorsqu’elle dirigeait la diplomatie américaine, le prétendant républicain s’est montré bien plus ouvert à une coopération avec le Kremlin.

Avril 2017. Quelques mois après ces événements, nous reprenons notre sac à dos, direction New York et Washington, pour rencontrer celles et ceux qui, dans les services de renseignement américains et les sociétés de cybersécurité, enquêtent sur ce dossier et, plus largement, sur le phénomène des fuites massives. C’est une gageure.

La publication des messageries du Parti démocrate a plongé le pays dans un véritable psychodrame politique. Rapports, contre-rapports et auditions spéciales du Sénat et de la Chambre des représentants se succèdent. Les médias américains multiplient les enquêtes sur une possible collusion entre le nouveau locataire de la Maison-Blanche, Donald Trump, et Vladimir Poutine, allant jusqu’à évoquer une potentielle complicité de l’équipe du Républicain dans le piratage des messageries du Parti démocrate. En retour,

Trump tire à boulets rouges sur la presse américaine, accusée de partialité. Le premier amendement de la Constitution américaine, qui garantit la liberté d'expression, et donc celle de la presse, est brandi tous les jours contre une présidence américaine qui se vit comme assiégée par les révélations sur ses liens avec l'appareil de sécurité russe. Et nous, simples journalistes français, arrivons comme des fleurs au milieu de ce chaos pour poser benoîtement des questions sur l'élément déclencheur de cette hystérie collective… L'accueil, on s'en doute, ne fut pas exactement à la hauteur de nos espérances.

Dans ce contexte incendiaire, certains de nos interlocuteurs, habituellement loquaces, ont soudain perdu leur faconde, se bornant à fustiger l'ingérence russe. D'autres, ouvertement républicains, nous ont confessé leur hébétude face à ce président issu de leurs propres rangs et désormais soupçonné de toutes les turpitudes. Même nos sources dans les services de renseignement américains sont subitement devenues muettes : en guerre ouverte contre la Maison-Blanche, elles ne voulaient pas prendre le risque de gaspiller les munitions patiemment accumulées contre Trump en en donnant la primeur à des journalistes français. À force de persévérance, certains observateurs privilégiés ont tout de même fini par s'ouvrir et nous permettre de pénétrer dans les arcanes de ce qui restera dans les annales de la diplomatie et du renseignement comme l'une des plus importantes opérations de déstabilisation contre les États-Unis.

Dans son grand bureau de Manhattan, un ancien ponte de la CIA, assis sous un tableau représentant des moudjahidines afghans combattant l'armée russe avec des armes fournies par l'agence du renseignement américaine – une des plus importantes opérations de l'histoire de l'agence, à laquelle notre interlocuteur a activement participé –, résume pour nous le point de vue de son ancien service : « C'est le grand retour de l'impérialisme russe, et c'est aujourd'hui la priorité numéro 1 du renseignement américain. »

À l'écouter mêler, dans un long monologue, ses souvenirs des années 1980 et les batailles contemporaines dans le cyberespace, nous comprenons que les espions sont nombreux, tant à Moscou qu'à Washington, à vouloir rejouer la guerre froide sur Internet. Des deux côtés du détroit de Béring, les stratèges du renseignement se désespèrent d'en être réduits à lutter contre le terrorisme djihadiste et rêvent de retrouver leur grandeur perdue ; les

batailles mondiales d'influence et de contre-influence leur manquent. Problème : en opposant deux idéologies, la guerre froide ouvrait le monde entier aux luttes américano-russes. Les deux superpuissances s'affrontaient par alliés interposés à travers la planète. La chute du mur de Berlin a mis fin à ces affrontements planétaires, ne laissant derrière elle que des conflits localisés et des guerres d'intérêt national. Le cyberespace ouvre un nouveau terrain de jeu aux chocs des empires.

À partir d'octobre 2016, puis surtout à partir de décembre, les services américains de renseignement, CIA en tête, affirment de plus en plus ouvertement, dans leurs rapports, que l'exécutif russe est directement lié à la cyberattaque qui a touché le Parti démocrate. L'opération aurait commencé, en juin, par une vaste campagne de hameçonnage sur les e-mails des principaux animateurs de la campagne démocrate, notamment sur la messagerie de John Podesta, le directeur de campagne de Hillary Clinton. On l'a vu, la technique dite de l'hameçonnage consiste à envoyer des courriels sous des prétextes fallacieux depuis de faux serveurs afin de récupérer les identifiants et les mots de passe des personnes visées. Pour le renseignement américain, qui publiera en janvier 2017 une enquête « hautement classifiée » sur le sujet, ce sont des hackers russes qui auraient piraté les messageries du Parti démocrate puis auraient ensuite blanchi les informations recueillies en les fournissant au site WikiLeaks.

Au total, entre le 10 mars et le 7 avril 2016, les Russes auraient ciblé 109 adresses électroniques de membres de la campagne de Hillary Clinton. Pas moins de 36 d'entre eux seraient tombés dans le piège numérique qui leur était tendu, ouvrant à la seconde une brèche dans le système du Parti démocrate. Une autre campagne d'hameçonnage, plus réduite, vise peu après quelques dizaines d'autres membres de la campagne. Les e-mails obtenus sont d'abord publiés sur un site anonyme, DCleaks.com, puis, cette plate-forme créée pour l'occasion se révélant insuffisamment référencée pour toucher un large public, ils sont vite transmis et diffusés sur le site de Julian Assange pour susciter alors la déflagration attendue. Sur la foi de l'enquête des services américains, WikiLeaks se voit rapidement accusé d'être un relais de la propagande russe. La réaction de Julian Assange sera particulièrement surprenante : il niera farouchement que la Russie soit à l'origine de cette fuite de données… alors que son site est précisément paramétré pour que ses administrateurs ne puissent savoir qui transmet des documents confidentiels à la plateforme. En affirmant que les services

russes ne lui ont pas fourni les mails du Parti démocrate, Assange met donc paradoxalement fin à l'anonymat absolu que le site prétend garantir à ses sources.

Après le piratage des messageries de son Comité national, le Parti démocrate a très vite demandé l'aide des autorités, FBI en tête, et de plusieurs sociétés de cybersécurité pour remonter jusqu'à l'origine de l'attaque. Pour l'une d'entre elles, Crowdstrike, l'attaque est signée Fancy Bear, un groupe de pirates dont les cyberlimiers de l'entreprise traquent les méfaits depuis 2014. Fancy Bear est une nébuleuse de hackers anonymes que les enquêteurs informatiques ont affublée de multiples sobriquets : APT28, Pawn Storm, ou encore Sofacy Group. Ce groupe apparaît comme l'un des principaux collectifs de hackers russes, travaillant en étroite collaboration avec le service de renseignement militaire de Moscou, le GRU.

*

Traqué par le renseignement américain et ses consultants, Fancy Bear, comme d'autres groupes, participe en réalité d'un système plus vaste, celui de la sous-traitance d'attaques informatiques par l'appareil de sécurité russe. Pour mener des piratages, et faire ensuite fuiter les documents obtenus, la Russie a laissé prospérer un environnement hybride de cyberrenseignement, très proche de celui adopté par Israël ou l'Inde, où services de renseignement et équipes de hackers indépendantes s'épaulent mutuellement. Le système russe, dont il est particulièrement difficile de démêler l'écheveau, n'est connu qu'à la marge par les services occidentaux de renseignement qui naviguent largement à vue dans les cybersteppes. En Russie même, c'est un sujet absolument tabou : toutes les sources russes que nous avons sollicitées pour cette enquête se sont immédiatement fermées quand elles ont compris l'objet de nos investigations. Signe de son importance stratégique, la nature des liens entretenus par le Kremlin avec le monde des hackers est une question que personne, et surtout pas les officiels, ne veut se risquer à aborder.

La structure de cyberrenseignement russe a beau être opaque, son but, lui, est avoué. Un rapport de la Defense Intelligence Agency (DIA), le service de renseignement du Pentagone, publié en juin 2017, souligne que,

« depuis au moins 2010, la doctrine militaire russe a fait du développement des forces et des moyens consacrés à la “confrontation informationnelle”, le concept russe visant à instaurer la suprématie dans les guerres médiatiques, une priorité. Et ce, en temps de paix comme en temps de guerre. La “confrontation informationnelle” porte à la fois sur le contrôle de l’information et sa dissémination ». Toujours selon le Pentagone, « les cyberopérations constituent une partie non négligeable des velléités russes du contrôle de l’environnement informationnel ». Cette doctrine est d’ailleurs décrite par les Russes eux-mêmes, qui remettent régulièrement à jour (2010, 2016) leurs objectifs stratégiques et publient les résultats.

Si les Russes ne cachent pas leur stratégie en matière de « suprématie informationnelle », leur méthode pour y parvenir est en revanche beaucoup plus obscure, et jalousement protégée. Si l’on en croit les rapports d’analyse et de synthèse du renseignement américain, le commandement russe en matière de cyberattaque serait proche de la pyramide hiérarchique parfaite. Tout en haut, le Kremlin déciderait de tout, tandis que les trois grands services de renseignement, le service de renseignement extérieur, le SVR, celui de l’intérieur, le FSB, et le service de renseignement militaire, le GRU, seraient chargés de mettre en musique et de transmettre les ordres de la présidence à des bataillons de « hackers patriotiques » disciplinés.

Un de nos interlocuteurs réguliers, un ancien officier du renseignement extérieur britannique, le MI6, bat en brèche cette analyse. Aussi brouillon que brillant, il a passé de nombreuses années à ausculter le vaste appareil russe de renseignement et de sécurité, d’abord pour la Couronne, puis, ensuite, pour des entreprises. Reconverti dans l’enquête privée, il a beaucoup travaillé sur des dossiers russes, et parfois même frayé avec les hackers du pays.

Un après-midi de juin, il a accepté de nous dévoiler les arcanes du hacking d’État : « Les médias américains ont tendance à présenter le système russe en la matière comme un tout homogène et bien construit. Or, pour le côtoyer de près, c’est plutôt un joyeux bordel. En réalité, chaque grande agence de renseignement, le service de sécurité intérieure (FSB), le renseignement extérieur (SVR) et le renseignement militaire (GRU) – pour lequel travaillerait Fancy Bear –, dispose d’équipes de hackers à sa botte. Certains de ces groupes informels travaillent même pour plusieurs services à la fois. Surtout, ce qu’on oublie souvent, c’est que ces grands services

sont en permanence en guerre entre eux, pour obtenir plus de fonds, plus de prérogatives, et pour plaire au grand patron du Kremlin. »

Ainsi, en fonction des demandes de l'autorité politique et de la mission, chacun de ces grands services contacte un groupe de hackers qu'il tient – plus ou moins – sous sa coupe. Dans cet environnement très concurrentiel, le FSB dispose d'un avantage décisif sur les autres agences : le service de sécurité intérieure a la charge de délivrer aux sociétés de cybersécurité et de cyberattaque les autorisations nécessaires pour opérer légalement dans le pays. Grâce à ce rôle de régulateur, il garde un œil sur les collaborateurs des services concurrents. À la condition, bien sûr, que ceux-ci soient dûment déclarés, ce qui n'est pas toujours le cas pour les opérations les plus discrètes…

De ce fait, nous relate un dirigeant retraité de la branche cyber d'un grand service européen de renseignement, « rien n'empêche un groupe de hackers de s'autosaisir d'une cible par zèle, pour plaire à son autorité de tutelle, qui, pensent-ils, sera ravi de recevoir un tel butin ». Ce que viendrait presque confirmer Vladimir Poutine, lorsqu'il a digressé, fin mai 2017, devant un parterre de dirigeants internationaux et de journalistes invités au Forum économique de Saint-Pétersbourg : « Les hackers sont des gens libres, juste comme des artistes qui se lèvent le matin de bonne humeur et commencent à peindre… », ajoutant dans un sourire : « S'ils sont patriotes, ils peuvent vouloir contribuer au combat contre ceux qui, pensent-ils, veulent du mal à la Russie. »

Notre interlocuteur britannique, spécialiste des services russes de renseignement, nous rappelle que cette figure de « hacker patriotique » systématiquement mise en avant par la propagande russe est largement un mythe, et qu'il faut plutôt lui substituer une réalité plus prosaïque : les pirates informatiques sont souvent « tenus » par les autorités russes, qui les ont généralement pris la main dans le sac plus tôt dans leur carrière, pour des activités banalement criminelles. En échange de missions menées pour l'État, les autorités leur accordent un blanc-seing pour continuer leurs cyberattaques de banques et d'entreprises, tant qu'elles ne visent pas des cibles russes. L'un des exemples les plus emblématiques de ce *modus vivendi* est la liberté dont jouit un certain Yevgeny Bogachev. Dans les années 2000, ce hacker a signé des cyberattaques criminelles particulièrement audacieuses, vidant les comptes de petites banques

américaines et faisant chanter les entreprises en verrouillant leur système informatique contre rançon. Toutes ces opérations étaient menées *via* un réseau planétaire d'ordinateurs infectés par ses virus – ce qu'on appelle un *botnet* –, une légion de disques durs zombies, prêts à servir ses intérêts et à relayer ses offensives. Après cette première carrière criminelle, Yevgeny Bogachev a brusquement élargi, au début des années 2010, ses activités au-delà du secteur financier. Les experts informatiques ont commencé à retrouver les traces des exploits de Bogachev dans des attaques visant des cibles dont il ne pouvait espérer retirer aucun bénéfice matériel, mais qui constituaient, en revanche, des priorités d'intérêt stratégique pour Moscou. Il est depuis 2014 sous le coup d'un mandat d'arrêt du FBI, qui offre trois millions de dollars pour toute information pouvant permettre sa capture. Fin 2016, peu avant son départ de la Maison-Blanche, Barack Obama a ordonné des sanctions financières contre lui. Pourtant, Bogachev coule des jours paisibles en Russie. Les autorités locales ne l'ont jamais appréhendé, et il vivrait tranquillement dans la station balnéaire d'Annapa, sur la mer Noire.

Ces hackers à la solde de Moscou n'hésitent d'ailleurs pas à se procurer certains de leurs outils sur le Darknet, où des pirates opérant pour les services russes ont pu acheter des lignes de codes à des cyberbricolos issus de pays adversaires de Moscou, notamment ukrainiens, voire américains !

Mais notre ami londonien nous met en garde : les pirates russes, si protégés soient-ils, ne sont pas tout-puissants. « On n'emploie des hackers que pour des opérations massives, indiscriminées et, finalement, assez basiques (hameçonnage massif, etc). Si, en revanche, on veut mener une opération de hacking très ciblée, sur une personne très précise, mieux vaut aller voir des Israéliens ou Indiens, bien meilleurs pour ces attaques sur mesure… »

La remarque, proférée sur un ton d'évidence, nous laisse sans voix : voilà six mois que nous progressons à tâtons dans les arcanes du hacking des pays dont il parle, persuadés qu'ils sont des centres mondiaux du piratage, et voilà qu'un interlocuteur, visiblement bien introduit dans ces milieux, nous lâche la confirmation que nous cherchions sans succès ailleurs. Le monde de l'enquête privée est visiblement très bien informé sur la gamme de services offerts par les hackers…

La coopération entre les agences russes de renseignement et les équipes de *freelance*, faite de petits arrangements entre criminels convaincus et

fonctionnaires pressés de présenter à leurs supérieurs des résultats mirobolants, a l'avantage d'être moins coûteuse en fonds publics qu'une belle et grande agence de renseignement technique, comme en disposent la plupart des démocraties occidentales, États-Unis en tête. Mais, au-delà de ses avantages pratiques, ce système permet également à l'État russe de nier toute implication dans une cyberattaque, puisqu'il s'est organisé pour n'avoir aucun lien formel avec l'équipe qui a pénétré les réseaux de l'adversaire, si jamais celle-ci est identifiée. Dans cet environnement de faux-semblants et de déni plausible, des groupes peuvent donc opérer en toute impunité.

*

Fancy Bear est probablement l'ensemble de pirates le plus étroitement encadré par l'appareil russe de cyberespionnage. Cette équipe de hackers, si elle est obscure, voire inconnue du grand public, empêche de dormir les bataillons de cyberenquêteurs de la CIA, du FBI et de la NSA. Car, même avant la fuite des mails du Parti démocrate, ce groupe a été associé à certaines des plus audacieuses opérations de fuite massive de données piratées de ces dernières années, toutes menées au nom de la guerre de l'information lancée par le Kremlin.

La lecture des rapports des sociétés de cybersécurité qui ont traqué pendant des mois, voire des années, Fancy Bear montre que ces pirates ont laissé des traces informatiques de leur implication dans de nombreuses opérations. Ainsi, le groupe a attaqué en août 2016, *via* une campagne de hameçonnage massive, les e-mails de l'Agence mondiale antidopage. Celle-ci avait eu le malheur de bannir la Russie de ses instances, après qu'une enquête avait révélé la consommation massive et organisée de produits interdits au sein de la Fédération d'athlétisme russe, avec l'aide des autorités. Le dossier a largement été relayé dans les pages « Sport » des grands quotidiens mondiaux et a donné lieu à une formidable passe d'armes entre les États-Unis et la Russie.

Comme nous l'avons relaté dans notre lettre d'information Intelligence Online, à la demande de l'Agence mondiale anti-dopage, ce sont d'anciens agents de renseignement britanniques et américains qui ont enquêté sur les réseaux d'approvisionnement en produits interdits des sportifs russes. Et ce,

avec des méthodes dignes de la guerre froide : ces anciens espions ont recruté des sources au sein même des administrations russes de formation et d'entraînement de sportifs de haut niveau et ont même réussi à retourner certains cadres du sport russe et à les amener, avec des précautions dignes d'un transfert d'espions, en Occident. En d'autres mots, ils ont réussi à créer des « transfuges sportifs », prêts à leur décrire la machine de dopage mise en place directement par les autorités de Moscou afin de dominer l'athlétisme mondial. La comparaison n'est pas seulement métaphorique : la distribution de produits dopants était contrôlée… par le service russe de renseignement intérieur, le FSB.

Sur la base des éléments récoltés par les enquêteurs anglo-saxons, l'Agence mondiale antidopage a finalement exclu la Russie en juillet 2016. Un mois plus tard, la messagerie de l'organisation était pénétrée par les hackers de Fancy Bear et un compte Twitter anonyme, baptisé Anonymous Poland, diffusait les e-mails piratés, révélant les négociations internes à l'organisation internationale ainsi que des données confidentielles portant sur d'autres sportifs. Une fuite massive en représailles à l'offensive américaine sur le sport russe, source de fierté et d'influence pour Moscou.

Et le schéma se reproduit quasi à l'identique en avril 2017, lorsque l'Association internationale des fédérations d'athlétisme (AIFA), qui a travaillé avec l'Agence mondiale antidopage sur le dossier russe, voit elle aussi ses messageries piratées. Après analyse, il s'agirait toujours du groupe Fancy Bear, même si l'attaque n'a pas – encore ? – donné lieu à une fuite massive…

Toutes ces prouesses ne représentent que la face émergée de la cyberlégion Fancy Bear. Au vu des nombreux rapports d'incidents régulièrement émis par les sociétés de cybersécurité, et minutieusement épluchés par nos soins, Fancy Bear ne fait fuiter les résultats de ses attaques que depuis quelques années, alors que le groupe mène des actions de piratage depuis bien plus longtemps.

Fancy Bear a commencé à opérer dès la fin des années 2000, notamment contre des gouvernements perçus comme hostiles à la Russie. Le groupe a coordonné l'assaut contre des réseaux gouvernementaux géorgiens au moment de la guerre entre Moscou et Tbilissi en 2008. L'OTAN a également subi une cyberattaque de Fancy Bear à cette période. Deux entreprises très liées au gouvernement américain, la société de services

militaires privés Academi (ex-Blackwater), spécialisée dans la fourniture de gardes armées aux diplomates et militaires américains en zone de guerre, ainsi que le sous-traitant des services de renseignement Science Applications International Corporation (SAIC), ont elles aussi été ciblées en 2008. Ces premières interventions de Fancy Bear étaient des piratages « classiques », seulement destinés à cyberimmobiliser l'ennemi ou à lui subtiliser des informations. Ce n'est qu'à l'orée des années 2010 que le collectif de hackers à la solde de l'État russe s'est lancé dans la publication du butin de ses piratages.

*

Tous les premiers exploits des hackers de Fancy Bear (Géorgie, OTAN, etc.) répondent à la problématique première du renseignement : collecter de l'information. Autrement dit mener des piratages et des intrusions dans les réseaux de l'adversaire en procédant avec la plus grande discrétion possible afin que la cible ne remarque même pas « l'emprunt » de ses données. Le but est de disposer d'un avantage comparatif : savoir ce que l'autre sait, sans que ce dernier sache que l'on sait. Le b.a.-ba de l'espionnage, en somme.

Tout change en 2010, une date qui marque une rupture pour l'appareil de sécurité russe et va inspirer une nouvelle doctrine et un nouveau mode opératoire. Cette année-là, en avril, juin et novembre, le site WikiLeaks, créé quatre ans plus tôt par Julian Assange dans le but avoué de publier des fuites massives, diffuse successivement des vidéos de bavures des troupes américaines en Irak, des rapports d'opérations sur la guerre en Afghanistan, puis en Irak, et, finalement, l'apothéose, 251 287 câbles diplomatiques du département d'État. Le retentissement est mondial, tous les journaux s'en emparent. WikiLeaks devient une marque, la référence mondiale de la fuite massive, et Julian Assange acquiert, grâce à ces trois publications, une véritable aura, celle d'un combattant de l'information prêt à affronter les grandes puissances du secret, États-Unis en tête.

La diplomatie américaine se trouve durablement déstabilisée, et les conséquences de l'opération sont étudiées de très près à Moscou. Voir la toute-puissance américaine ébranlée par une « simple » fuite de données ouvre des perspectives inédites aux stratèges du Kremlin : se pourrait-il que

les opérations de piratage qu'il mène depuis des années puissent se transformer en arme de déstabilisation massive ?

Cette intuition se cristallise trois ans plus tard, à l'occasion d'une diffusion de données encore plus sensibles que les télégrammes diplomatiques américains, car elle touche à ce que les États ont de plus secret. À partir du 6 juin 2013, Edward Snowden, un ancien sous-traitant de la NSA, l'agence américaine en charge de la surveillance des réseaux de télécommunication, transmet au quotidien britannique *The Guardian* puis au *New York Times* des milliers de documents internes de la communauté américaine du renseignement. Au total, il aurait subtilisé à son ancien employeur près de 1,7 million de fichiers. Un recel comme n'en a jamais subi aucun service de renseignement dans le monde. Cette fuite va plonger la principale agence visée, la NSA, dans la tourmente. Accusée de surveiller tout le monde et tout un chacun, l'agence est ébranlée jusque dans ses fondements. Un simple administrateur-réseau est en train de mettre à genou la colonne vertébrale de l'hyperpuissance mondiale. Sous l'œil et pour le plus grand plaisir du Kremlin.

Passés maîtres dans l'art de l'espionnage, les services russes du renseignement décident de changer de paradigme. Un vieux briscard d'un service de cyberrenseignement européen, avec qui nous déjeunons à Paris au printemps 2017, nous glisse ainsi que, « avec WikiLeaks et Snowden, les Russes comprennent très vite que diffuser massivement les e-mails d'une organisation ou d'un gouvernement peut amener, en quelques clics, à plus de résultats diplomatiques en quelques jours qu'un agent infiltré chez l'ennemi pendant des dizaines d'années ».

Malgré ses racines anciennes, la technique de la fuite massive de données passe encore mal chez les vétérans de l'espionnage, en Russie et ailleurs, tant elle défie l'une des règles fondamentales du renseignement : opérer incognito et ne jamais laisser l'adversaire comprendre que l'on intercepte ses communications. Ainsi, cet ancien du renseignement technique israélien, que nous avions rencontré en avril à Tel Aviv, peine à s'adapter : questionné sur l'utilité des fuites massives d'e-mails pour affaiblir un pays ennemi, il refuse obstinément de considérer qu'il s'agit d'une tactique valide : « Le premier but d'un service de renseignement, c'est d'infiltrer ses ennemis et de préserver au maximum ses accès secrets. Organiser une fuite

massive de documents serait, de ce point de vue, totalement contre-productif. » Mais ces préventions n'ont plus cours dans un monde où l'information, comme les opinions publiques, est de plus en plus globalisée. Et où l'impératif de discrétion a été remplacé par le déni plausible : les piratages massifs étant systématiquement menés par des hackers, les États peuvent toujours nier toute implication, comme le fait la Russie pour l'intrusion dans les messageries du Parti démocrate.

Coïncidence ? En 2013-2014, alors que le Kremlin prend conscience de la nouvelle dimension prise par la guerre informationnelle, le groupe Fancy Bear modifie sa manière d'opérer. L'équipe, qui a toujours mené des intrusions informatiques discrètes, gardant pour elle-même, ou ses commanditaires, les informations récoltées, commence à les diffuser. Le groupe va s'essayer d'abord à des publications sur des sites anonymes, retransmis notamment *via* des comptes Twitter, anonymes eux aussi. Ainsi, les données subtilisées sur les réseaux du Parti démocrate seront tout d'abord mises en ligne sur un site créé pour l'occasion, DCleaks.com. Sauf que le site, mal référencé, n'a aucun retentissement.

Fancy Bear trouve alors un autre véhicule pour mener ces opérations : la plateforme WikiLeaks, déjà mondialement connue. Le site de Julian Assange dispose de toutes les caractéristiques que Moscou recherche : il assure garantir l'anonymat de ses contributeurs, il est auréolé du prestige de la publication des télégrammes diplomatiques américains – fournis par un lanceur d'alerte sincère et courageux, Bradley Manning – et il tient un discours anti-impérialiste. Le rapprochement entre le Kremlin et WikiLeaks va être facilité par la personnalité de son leader charismatique, Julian Assange, dont la soif de célébrité constitue un formidable vecteur de recrutement.

Petit à petit, grâce à WikiLeaks, que ce dernier en soit conscient ou non, Moscou a pu dévoyer le concept originel de la fuite massive de données et de la figure du lanceur d'alerte, afin de parfaire son formidable arsenal de déstabilisation massive. L'apothéose de cette stratégie sera le piratage du Parti démocrate en 2016.

Le site de Julian Assange, inventeur de la fuite massive de données moderne et surtout de la marque « Leak », a joué un rôle central dans

la campagne du Kremlin. Il a permis d'anonymiser, de légitimer, puis de diffuser largement les documents récupérés lors de piratages sponsorisés par Moscou. Pour la plupart de nos interlocuteurs, la cause est entendue : le charismatique dirigeant du site, Julian Assange, est devenu un agent à la solde du Kremlin.

Au moment même de notre séjour à Washington, le nouveau patron de la CIA, Mike Pompeo, a choisi, pour sa première intervention publique, le 13 avril 2017, dans la capitale américaine, d'attaquer frontalement l'organisation de Julian Assange en des termes particulièrement virulents. « WikiLeaks se conduit comme un service de renseignement hostile et s'exprime comme un service de renseignement hostile », déclarera Pompeo devant un parterre de diplomates peu habitués à entendre le directeur de la première agence de renseignement du monde s'exprimer de manière aussi directe. « WikiLeaks a encouragé ses partisans à faire acte de candidature à la CIA pour lui procurer des documents classifiés. WikiLeaks a encouragé et aidé Bradley Manning à voler des informations secrètes. Et WikiLeaks concentre presque exclusivement ses attaques sur les États-Unis, tout en recevant le soutien de pays et d'organisations non démocratiques. Il est temps d'appeler WikiLeaks par son nom : c'est un service de renseignement non étatique hostile aux États-Unis et encouragé par des États comme la Russie. »

La charge, lapidaire, n'est pas sans justifications. Assange, fervent anti-impérialiste et doté d'un ego surdimensionné, semble s'être peu à peu laissé déborder, au point d'avoir épousé les vues de Moscou, tant par intérêt personnel que par convergence idéologique.

Car Assange constitue une proie idéale pour un service de renseignement. Pour cibler une recrue, un service travaille toujours à partir des failles de l'individu visé. Au nombre de quatre, elles sont désignées en anglais par l'acronyme MICE, pour « Money – Ideology – Compromise – Ego ». Autrement dit : un individu peut être persuadé de coopérer soit par la promesse d'argent, la convergence idéologique, la menace de voir sa réputation entachée par des révélations compromettantes ou bien tout simplement en flattant son ego. Animé de sentiments anti-impérialistes très vifs, Assange pouvait facilement faire l'objet d'une approche idéologique. Mais le fondateur de WikiLeaks cochait une deuxième case sur la liste de la recrue idéale : il a une très haute idée de lui-même et est d'une

susceptibilité presque maladive quand on touche à sa réputation et à son image, celle d'un combattant solitaire en guerre contre les administrations mondiales du secret. Toute critique à son encontre, toute tentative, même fugitive, de le concurrencer sur son créneau suscite de sa part une réaction immédiate, et immanquablement violente.

À ce tableau déjà prometteur pour les professionnels de la manipulation est venue s'ajouter une troisième faiblesse : l'argent. Dès 2010, les États-Unis ont fait fermer un à un tous les comptes bancaires de WikiLeaks, et l'organisation, qui ne vit que de dons, ne peut plus opérer de levée de fonds. Les représailles de Washington contre le héraut de la transparence auront paradoxalement accéléré son alignement sur les intérêts russes.

Le rapprochement tant idéologique que tactique entre WikiLeaks et la Russie s'est effectué en plusieurs étapes. Il commence en 2010, peu avant la publication par le site de la base de données des télégrammes diplomatiques américains. À cette période, Assange s'inquiète des accusations de partialité qui le visent et veut, après avoir exposé l'administration américaine, publier une fuite massive sur la Russie. Il multiplie les annonces sibyllines et enregistre même un nouveau site Internet baptisé RULeaks.org. Dès l'été 2010, un affidé de Moscou fait son apparition dans l'entourage d'Assange. Il s'agit d'Israël Shamir, un éditorialiste régulièrement accusé d'antisémitisme qui a table ouverte dans les médias d'État russes. Rapidement, Shamir devient le « représentant de WikiLeaks en Russie » : il partage avec Assange une rhétorique fiévreusement anti-impérialiste. L'éditorialiste fait profiter la Russie de sa proximité avec WikiLeaks : selon l'Allemand Daniel Domscheit-Berg, un ancien proche collaborateur d'Assange, Shamir obtient, avant leur publication, des copies d'une partie des télégrammes diplomatiques américains, qu'il emporte avec lui en Biélorussie, puis en Russie. Certains de ces documents seront publiés dans le magazine *Russian Reporter*, proche du Kremlin. Minsk, pour sa part, utilisera les autres pour mener une virulente campagne contre ses opposants.

Au même moment, Julian Assange est accusé de délits sexuels en Suède et visé par un mandat d'extradition. Il refuse de s'y plier, criant au complot américain, et juge qu'en répondant aux convocations de Stockholm il court le risque d'être déféré aux États-Unis, où les autorités cherchent à le mettre

en examen pour complicité d'espionnage. Moscou s'engouffre dans la brèche. Israël Shamir, toujours lui, publie deux articles dans un tabloïd de gauche américain, *Counterpunch*, accusant les deux femmes qui ont porté plainte contre Assange pour rapports sexuels non consentis et non protégés d'avoir piégé le fondateur de WikiLeaks pour le compte des États-Unis. Le propre fils de Shamir, le journaliste suédois Johannes Wahlström, est le témoin de moralité d'Assange face aux autorités judiciaires suédoises, mais, contrairement à son père, il n'attaquera pas publiquement les deux accusatrices.

En revanche, Wahlström joue les intermédiaires entre Assange et la télévision d'État russe RT. Conscient des difficultés financières de WikiLeaks, le fils d'Israël Shamir suggère à son fondateur d'animer, contre rémunération, une émission de télévision sur la chaîne. « The Julian Assange Show » compte douze épisodes, diffusés de janvier à juillet 2012. Le programme est produit par RT, mais a vocation à être distribué sur d'autres chaînes. La demande est forte, mais RT ne fera rien pour vendre les droits du « Julian Assange Show ». Les honoraires permettent à Assange, qui a essayé sans succès d'écrire une autobiographie, d'améliorer sa situation financière. Sur le plateau de RT, il interviewe successivement le philosophe slovène Slavoj Žižek, le Secrétaire général du parti chiite Hezbollah, Hassan Nasrallah, mais surtout, le 21 mai 2012, le président équatorien Rafael Correa, allié fidèle du régime de Vladimir Poutine. Moins d'un mois plus tard, le 19 juin 2012, celui-ci lui offre l'asile politique dans l'ambassade de son pays à Londres afin de permettre à Assange d'échapper aux poursuites intentées contre lui par la Suède et, potentiellement, par les États-Unis.

À l'été 2012, Assange est donc protégé par un gouvernement lié à la Russie et perçoit des subsides de la télévision d'État russe. À partir de cette date, il va insensiblement intégrer l'appareil d'influence de Moscou. Toutes les fuites massives publiées par WikiLeaks ciblent uniquement les États-Unis, et jamais la Russie. Mieux, en juin 2013, WikiLeaks joue un rôle déterminant dans l'opération d'aiguillage d'Edward Snowden vers Moscou. Réfugié à Hong Kong et activement recherché par les États-Unis, l'ancien sous-traitant de la National Security Agency cherche désespérément une échappatoire. Julian Assange demande à l'Équateur de lui accorder l'asile et dépêche à ses côtés sa compagne occasionnelle, Sarah Harrison, qui convainc Snowden de gagner Quito *via* Moscou et La Havane. Mais

Snowden ne va pas plus loin que la Russie, permettant au régime de Vladimir Poutine de se poser en défenseur de la liberté d'expression, une position pour le moins paradoxale…

Cette association permet à Assange de survivre, puis, peu à peu, de revenir dans la lumière. Après le scandale mondial qu'a constitué la publication des télégrammes diplomatiques américains, WikiLeaks a traversé une période creuse, ne diffusant plus que des documents d'importance mineure, voire de simples archives. En parallèle, plusieurs cadres historiques de WikiLeaks ont rompu avec l'organisation, jugeant Assange mégalomane et de plus en plus dictatorial. Mais, en 2015, WikiLeaks renaît de ses cendres et publie plusieurs documents internes à la NSA qui montrent que l'agence d'interception américaine a écouté le président français et plusieurs leaders politiques européens. L'année suivante, WikiLeaks tente de torpiller la candidature présidentielle de Hillary Clinton, violemment antirusse, en publiant les messages internes de son parti sur son site.

Les coïncidences récurrentes entre les publications de WikiLeaks et les objectifs diplomatiques de Moscou ne laissent pas de surprendre. Ainsi, en février 2017, la tension monte entre l'Occident et la Russie. À la suite du piratage de la messagerie du Parti démocrate, de plus en plus de voix plaident aux États-Unis pour des mesures de rétorsion contre l'ingérence russe. Les services de renseignement de plusieurs pays européens, France en tête, commencent à alerter leurs opinions publiques sur de possibles tentatives russes d'interférer dans leurs processus électoraux à venir (élection présidentielle en France, consultations parlementaires au Royaume-Uni et Allemagne).

C'est à ce moment précis que WikiLeaks diffuse un document, notamment dans le journal *Libération*, le 16 février, qui prouve que la CIA a espionné l'élection présidentielle française de 2012. Ce document est parfaitement authentique, mais sa publication permet à Moscou de répondre aux accusations américaines : il montre en effet que l'ingérence dans les processus électoraux n'est pas l'apanage des Russes. Le lendemain de la parution de l'article, le ministre des Affaires étrangères, Sergueï Lavrov, pourra ainsi parader à Munich, lors d'un sommet sur la sécurité européenne, et renvoyer les journalistes qui l'interrogent sur l'éventuelle participation de la Russie au piratage de l'élection américaine, au document publié par le

journal français, non sans souligner que les États-Unis devraient balayer devant leur porte avant d'accuser les autres…

Le problème, selon nos informations, c'est que WikiLeaks disposait du document de la CIA depuis plus d'un an et que Julian Assange se refusait obstinément à le publier, malgré son authenticité, et faisait lanterner ses cadres, qui ne comprenaient pas cette valse-hésitation. WikiLeaks ne rend public le document de la CIA que lorsque Moscou en a besoin, signant par là même son tropisme.

Mieux : au moment même où il divulguait les e-mails du Parti démocrate américain, Assange aurait refusé une contribution anonyme de près de 68 giga-octets de documents confidentiels russes ! L'un des activistes qui ont proposé ces données à WikiLeaks a raconté, en août 2017, au site d'information international Foreign Policy la fin de non-recevoir que lui avait opposée Assange. Selon nos informations, cet incident a suscité une gêne considérable au sein de l'organisation. Car celle-ci a déjà été accusée de sélectionner les documents qu'elle publiait en fonction de ses intérêts. En 2012, lorsqu'il a divulgué près de deux millions d'e-mails échangés par la nomenklatura syrienne, WikiLeaks aurait volontairement omis certains documents portant sur des accords financiers syro-russes. Cette révélation, portée devant une cour de justice new-yorkaise en septembre 2016, est relayée par les hackers activistes qui ont pénétré les réseaux syriens et fourni la base de données publiée par WikiLeaks !

L'organisation nie avec la dernière énergie toute forme de censure, mais Julian Assange prend la mesure du danger. Attentif à tout ce qui peut entacher sa réputation personnelle, il comprend que ces accusations récurrentes de collusion avec Moscou deviennent problématiques et, en propagandiste chevronné, allume un contre-feu. Le 19 septembre 2017, il commence à publier, sous le nom de « Spy Files Russia », une série de documents sur les principales entreprises de surveillance électronique russes. Problème : les archives mises en ligne sont loin d'être confidentielles ! Certaines sont des documents publiés par les sociétés elles-mêmes tandis que d'autres, les plus techniques, avaient déjà fuité auprès de journalistes, russes et occidentaux, plusieurs mois auparavant. Jugeant leur contenu peu significatif, ceux-ci n'en avaient rien fait : les pièces publiées par WikiLeaks ne font en effet pas référence aux services de renseignement russes, pourtant au cœur du système de surveillance d'Internet. Les

entreprises exposées par WikiLeaks vendent des outils de *deep-packet inspection*, une technique d'interception des flux digitaux pratiquée partout dans le monde et très peu confidentielle. Peu spectaculaires, les révélations du site de Julian Assange ne seront relayées que par deux médias européens, *La Republicca* en Italie et Mediapart en France, chacun des deux journaux prenant soin de préciser que les documents « sont, pour WikiLeaks, une réponse à ceux qui lui reprochent sa trop grande proximité supposée avec les autorités russes ».

Outre Julian Assange, Moscou peut compter sur un autre soutien de poids : Edward Snowden. Depuis ses révélations sur le fonctionnement et les outils de la NSA, celui-ci est « réfugié » en Russie. S'il a toujours nié avoir voulu s'établir dans ce pays, c'est néanmoins depuis Moscou qu'il continue son combat pour promouvoir la fin des programmes de surveillance de masse mis en place par son ancien employeur. Sa petite amie, Lindsay Mills, vit dans la capitale russe avec lui. Ce qui ne laisse pas de susciter moult interrogations, et un paradoxe majeur : comment promouvoir la transparence depuis un pays de plus en plus autoritaire ?

Avant nous, les deux journalistes russes les plus informés sur l'appareil de cybersécurité du pays, Andrei Soldatov et Irina Borogan, se sont aussi interrogés sur la place de Snowden dans la stratégie du Kremlin, dans un formidable livre, *The Red Web*. Paru en 2015 aux États-Unis aux éditions PublicAffairs (hélas non traduit en français), l'ouvrage est entièrement consacré au système russe de surveillance d'Internet. Les deux auteurs y notent un point largement passé inaperçu dans les médias occidentaux : l'arrivée de Snowden a permis à Vladimir Poutine de gérer un épineux dossier de politique intérieure. En juin 2013, au moment où l'ex-consultant de la NSA américaine atterrit à l'aéroport de Moscou, le pouvoir russe vient de lancer l'une de ses plus grandes offensives sur l'Internet, notamment sur les sites d'opposition. L'agence de contrôle des communications, donc du Web, Roskomnadzor, aidée par des supplétifs autoproclamés, la Ligue des cybergardiens d'un Internet sain, financée par des hommes d'affaires nationalistes, fait la chasse aux cyberopposants. Dans ce contexte, accueillir Snowden est un coup de communication magistral : comment accuser le Kremlin d'agir contre la liberté sur Internet quand le symbole même de la lutte contre la surveillance est accueilli à Moscou ? Mieux : les révélations

de Snowden fournissent au Kremlin le prétexte idéal pour intensifier la surveillance du Web. Si, comme le montrent les documents subtilisés par Snowden, Internet est massivement infiltré par l'agence américaine de surveillance des télécommunications, contrôler et protéger les réseaux russes devient un enjeu de souveraineté nationale, et non plus une censure de l'opposition… Soldatov et Borogan concluent : « Snowden ne savait peut-être pas ou n'a pas réalisé, mais ses révélations ont en réalité enhardi ceux qui en Russie réclamaient plus de surveillance d'Internet. » Le contrôle de l'État sur l'Internet russe s'est encore accru, avec de nouvelles mesures répressives votées ou décidées quasiment chaque année depuis lors. Snowden ne s'est jamais exprimé sur ce sujet.

Le pourfendeur de la NSA a même participé à une émission à la télévision russe avec Vladimir Poutine, en avril 2014, et lui a benoîtement demandé : « Est-ce que la Russie intercepte, conserve et analyse de quelque manière que ce soit les communications de millions d'individus ? Croyez-vous que l'argument d'augmenter l'efficacité des services de renseignement justifie de placer des sociétés entières sous surveillance ? Merci. » Ce à quoi le leader russe, après avoir plaisanté avec Snowden sur leur passé commun d'agents de renseignement, a simplement répondu : « Il n'y a pas, et ne peut pas y avoir, de surveillance massive [d'Internet en Russie – *NDA*] », notamment parce que la Russie « n'a pas de capacités techniques comme celles des États-Unis »… L'argument sera repris mot à mot par Snowden trois ans plus tard dans une interview menée le 11 septembre 2017 par le journaliste américain Jeremy Scanhill. Interrogé sur l'éventuelle participation de la Russie au piratage des messageries du Parti démocrate américain, le jeune homme répond : « Ces accusations donnent trop d'importance aux capacités techniques de la Russie. »

Ayant obtenu l'asile du Kremlin, Snowden a toujours refusé de parler à des journalistes russes, réservant ses interventions aux audiences occidentales, pour y détailler la mainmise du renseignement américain sur leurs démocraties. Aucune critique, en revanche, sur la surveillance pratiquée par la Russie. « Au moment où Snowden était à Moscou, la Russie était déjà en train d'essayer de changer les règles de l'Internet. Mais cela aussi a semblé échapper à l'attention de Snowden », concluent Soldatov et Borogan.

Le Kremlin a compris tout de suite l'intérêt de récupérer Snowden. Lorsque celui-ci a posé le pied à l'aéroport de Sheremetyevo, une équipe du FSB, le service de renseignement intérieur, était là, à l'attendre. Durant son transit en zone internationale, toutes les conférences de presse du consultant américain et ses (rares) contacts avec les journalistes étrangers étaient chaperonnés par le FSB. Très vite, un homme est apparu aux côtés de l'ancien sous-traitant de la NSA : l'avocat Anatoly Kucherena. Devenu le conseil juridique de Snowden, il a obtenu pour son client un permis de séjour russe, dont il brandit triomphalement le récépissé lors de la dernière conférence de presse de Snowden à Sheremetyevo. Or, outre ses activités d'avocat, Kucherena est aussi membre du conseil public du FSB…

Snowden a toujours clamé que Moscou n'était qu'une étape et que son véritable objectif était de s'établir en Amérique du Sud. Aucun des agents de renseignement occidentaux, américains, français ou britanniques que nous avons pu rencontrer et qui ont travaillé sur son dossier, ne croit ses déclarations : à partir de Hong Kong, cela n'a strictement aucun sens de partir vers Moscou pour gagner un pays latino-américain.

Il est peu vraisemblable que Snowden ait été recruté par la Russie quand il travaillait encore pour la NSA. Ainsi qu'on nous l'a relaté à New York comme à Washington, les agences américaines de renseignement ont tout fait pour établir un lien entre leur ancien sous-traitant et des agents étrangers, mais ont jusqu'à présent fait chou blanc. Dans la très longue enquête sur la défection de Snowden menée par le Congrès américain en décembre 2016, le chapitre sur l'aide qu'il aurait pu recevoir d'un État étranger pour dupliquer les documents de la NSA fait vingt lignes, toutes soigneusement noircies pour les lecteurs non habilités…

Seule certitude pour les enquêteurs parlementaires américains : en juin 2016, « un vice-président de la Commission de la défense du Parlement russe » a déclaré que Snowden « avait partagé des informations avec le gouvernement russe ». Le premier vice-président de ce comité, Andrei Krasov, qualifiera cette assertion de « blabla ».

Le fait d'avoir vraisemblablement agi seul ne dispense pas Snowden, une fois réfugié à Moscou, d'être devenu le parfait « idiot utile » du régime russe, comme l'a théorisé un lointain prédécesseur de Poutine, un certain Vladimir Ilitch Oulianov, dit Lénine. Snowden n'en a peut-être pas

conscience, mais il est l'un des principaux atouts du Kremlin dans un jeu qui le dépasse. Chaque jour qu'il passe à Moscou fait de lui une marionnette.

Moscou s'offrira même le luxe de transformer Edward Snowden en légende hollywoodienne. Interviewant Oliver Stone pour le magazine *Vanity Fair*, l'un de nous aura la surprise d'entendre le cinéaste américain raconter que c'est à l'origine l'avocat russe de Snowden, le conseiller du FSB Anatoly Kucherena, qui l'a contacté pour lui proposer de consacrer un film à l'ancien sous-traitant de la NSA. Mieux : ce film, sorti en septembre 2016 sous le titre *Snowden*, est partiellement fondé sur la version personnelle de Kucherena et résumée dans un roman, *Le Temps de la pieuvre*, publié en Russie mais non traduit ailleurs. *Snowden*, produit hors des États-Unis avec de l'argent allemand, se clôt sur quelques séquences documentaires où l'on voit le véritable Edward Snowden vivre paisiblement en Russie dans une confortable datcha avec sa petite amie. L'année suivante, Oliver Stone consacre un documentaire à Vladimir Poutine, qu'il interviewe longuement et complaisamment.

Installé dans son immense bureau qui domine Manhattan, un ancien vétéran de la Direction des opérations de la CIA – le cœur des opérations les plus clandestines de l'agence – nous glisse, un sourire aux lèvres, que les meilleures sources recrutées par un service de renseignement sont « les personnes convaincues d'agir pour le Bien et celles qui servent vos intérêts en croyant suivre les leurs ». À méditer.

* * *

Après avoir détourné la divulgation massive de données, les stratèges russes se seraient-ils mis en tête de subvertir le concept même de lanceur d'alerte ? C'est la question que pose une étrange affaire révélée par notre publication, Intelligence Online, et reprise ensuite dans la plupart des grands quotidiens anglo-saxons.

Mai 2017. Plusieurs sources nous indiquent que les services de renseignement occidentaux s'intéressent de très près aux élections législatives qui vont bientôt avoir lieu sur l'île de Malte, ébranlée par

plusieurs affaires de fuites massives. Effectivement, à cette période, la petite île, qui verrouille l'accès à l'est de la Méditerranée, est secouée par une série de révélations sur de possibles malversations commises par l'entourage du Premier ministre, Joseph Muscat, en lice pour sa réélection. En pleine campagne électorale, sa femme, Michelle Muscat, ainsi que son chef de cabinet, Keith Schembri, se sont vu accuser par l'opposition de détournement de fonds. Il est reproché à Schembri d'être l'actionnaire d'une société aux îles Vierges britanniques, qui lui aurait servi à blanchir des fonds. Celui-ci, ancien homme d'affaires, nie que ces activités aient pu être illégales. Peu après, la femme du Premier ministre Joseph Muscat est, elle aussi, accusée de bénéficier des largesses d'une société offshore, Egrant Inc., alimentée par la famille d'Ilham Aliyev, le président au pouvoir en Azerbaïdjan. Le couple Muscat réfute en bloc ces accusations, relayées par la journaliste indépendante Daphne Caruana Galizia dans plusieurs quotidiens maltais.

Or, en remontant à la source des informations visant les dirigeants maltais, on remarque que celles-ci sont émises par un mystérieux lanceur d'alerte, soigneusement protégé par les médias locaux et qui prétend risquer sa vie pour avoir dénoncé ces agissements – pour la plupart non corroborés. Ses révélations ont coïncidé, à partir du mois de mai, avec une fuite massive des données du registre des entreprises maltaises dans la presse occidentale. Cette base de données a été fournie anonymement à un consortium de journaux européens, l'European Investigative Collaborations (EIC, représenté par Mediapart en France), qui l'a publiée en feuilleton.

Selon nos informations, les services britanniques et américains se sont fortement penchés sur ce mystérieux lanceur d'alerte. Son identité et ses connexions personnelles donnent en effet un éclairage tout différent à l'affaire. Il s'agit en réalité d'une femme, de nationalité russe, nommée Maria E. Longtemps basée à Chypre, la plateforme offshore privilégiée par les oligarques russes, elle est comptable de formation. Relocalisée à Malte, elle a notamment exercé pour la Pilatus Bank, avant de travailler aujourd'hui pour une société sans objet commercial bien défini, Mtacc Ltd., qui appartient à un autre citoyen russe, Alex Zaslavsky, avec qui elle partage d'ailleurs son appartement. Ce dernier serait un familier de l'ambassade russe à La Valette, la capitale maltaise.

Les soupçons s’accumulent sur le couple, soupçonné d’entretenir des liens étroits avec la Russie. Les autorités maltaises, aiguillées par les services britanniques, confisquent le passeport de Maria E., une décision immédiatement dénoncée par l’ambassadeur russe sur place.

Pourquoi le Kremlin aurait-il encouragé une lanceuse d’alerte autoproclamée à opérer une fuite massive dans une île seulement connue pour ses sites touristiques et sa fiscalité ? Le Premier ministre maltais, après la publication de notre article dans Intelligence Online, a lui-même publiquement reconnu que les services de renseignement de pays alliés l’avaient alerté d’une volonté russe de perturber les élections législatives. Cette opération est intervenue en effet peu après que Joseph Muscat s’était frontalement opposé aux intérêts de Moscou en Méditerranée. Le Premier ministre maltais a refusé que les navires russes croisant au large de Malte pour rejoindre le théâtre d’opérations syro-irakien puissent se ravitailler en carburant sur l’île. Et ce, à la grande fureur du Kremlin, qui avait un besoin vital d’un point d’approvisionnement pour maintenir son pont maritime vers le Levant.

Le Premier ministre Dmitri Medvedev a publiquement fait part de son mécontentement lorsque Malte a refusé, en novembre, que le tanker *RFS Dubra*, qui accompagnait la *task force* du porte-avions *Amiral Kouznetsov*, puisse remplir ses cuves à Malte. Le ministère russe des Affaires étrangères avait même condamné la décision maltaise et, dans un communiqué, affirmé que Malte « avait été victime de la guerre de l’information menée par l’Occident ». De là à ce que le Kremlin se lance dans une vaste contre-attaque sur le même terrain, il n’y a qu’un pas… L’affaire se terminera de manière aussi tragique que mystérieuse : le 16 octobre, la voiture de Daphne Caruana Galizia, la journaliste qui a relayé les accusations de Maria E. contre les dirigeants maltais, sera détruite par une bombe et sa propriétaire tuée sur le coup.

IV

Géopolitique de la fuite massive

Emboîtant le pas à Moscou, d’autres États ont ajouté les diffusions massives d’informations confidentielles à leur arsenal de déstabilisation. Au point que dans certaines régions, tout particulièrement au Moyen-Orient, leur utilisation s’est généralisée dans toutes les batailles d’influence que se livrent les puissances locales.

Le 19 juin 2015, des dizaines de milliers d’e-mails rédigés par des diplomates saoudiens sont publiés par WikiLeaks. Ces messages, initialement publiés sur un petit site anonyme, wikisaleaks.com, révèlent petits et grands secrets de la politique étrangère du royaume wahhabite : comment Riyad achète les journaux et les politiques libanais, comment le royaume use de l’arme religieuse pour étendre son influence dans le monde, etc. Les e-mails sont un précipité des opérations d’influence que l’Arabie s’efforce de mener depuis plusieurs années, en particulier depuis l’émergence du « printemps arabe », en 2011. En 2010, le ministère saoudien des Affaires étrangères avait déjà été déstabilisé par les télégrammes diplomatiques américains publiés par WikiLeaks : dans leur correspondance, les ambassadeurs américains étrillaient le pouvoir saoudien.

Deux ans plus tard, en 2012, les serveurs de la compagnie nationale pétrolière, l’Aramco, avaient été ciblés par une attaque informatique. La fuite des e-mails de la diplomatie saoudienne est très rapidement revendiquée par une mystérieuse Yemen Cyber Army. Bien sûr, le Yémen ne possède pas d’armée électronique – voire pas d’armée du tout, diront les mauvaises langues. Et le pays figure systématiquement en queue des classements du taux d’accès à Internet.

Le contexte dans lequel intervient cette fuite de données a son importance pour comprendre les intérêts en jeu. En mars 2015, soit quatre mois avant la diffusion des messages électroniques de ses diplomates, l'Arabie saoudite, accompagnée par une coalition de pays arabes, est entrée en guerre au Yémen contre un groupe rebelle, les Houthis. Ceux-ci contrôlent depuis plusieurs mois certaines des zones les plus stratégiques du pays, notamment sa capitale Sanaa. Or les Houthis sont de confession zaydite, une branche du chiisme, et sont activement soutenus par l'Iran, qui conteste à l'Arabie son leadership régional.

Très curieusement, aucune enquête publique n'a été commanditée, ni par l'Arabie ni par ses alliés, pour trouver l'origine de la fuite massive qui a frappé la diplomatie saoudienne. Cependant, pour plusieurs de nos interlocuteurs, qui ont passé plusieurs années à observer, voire infiltrer, le cyberarsenal iranien, il ne fait guère de doute que Téhéran est derrière l'opération.

Il faut dire que l'Iran a considérablement développé, ces dernières années, ses capacités de cyberrenseignement. Le régime étant la cible numéro 1 de deux des plus puissants services de renseignement du monde, le Mossad israélien et la CIA, les maîtres espions du ministère du Renseignement et leurs homologues des Gardiens de la révolution ont dû déployer des trésors d'ingéniosité pour riposter aux cyberinfiltrations, voire aux cyberattaques, menées par leurs ennemis.

Pour ce faire, Téhéran a mis sur pied, de manière empirique, un système de cyberrenseignement assez proche de celui de son allié russe, mêlant techniciens d'État et équipes de pirates locaux. L'une d'entre elles s'est baptisée l'Iran Cyber Army ; contrairement à ce que son nom semble indiquer, il ne s'agit pas d'un corps d'armée ordinaire, mais plutôt d'un groupe de hackers placé sous la tutelle des pasdarans, les puissants Gardiens de la révolution de la République islamique d'Iran, qui ne répondent qu'au guide suprême Ali Khamenei. On retrouve l'organisation derrière plusieurs attaques informatiques. Ainsi, le renseignement américain lui attribue une intrusion, en 2012, dans les réseaux de l'Agence internationale d'énergie atomique (AIEA), menée au nom d'un faux nez, Parastoo.

Sous la pression des attaques américano-israéliennes, Téhéran a fait des progrès rapides en matière de cyberguerre. Dans un rapport publié fin

juillet 2017, la société israélienne de cybersécurité Clearsky soupçonne même l'Iran d'être derrière le groupe CopyKittens, qui aurait monté toute une architecture de hacking, disposant de relais aux États-Unis, aux Pays-Bas et en Russie. La firme a retrouvé les traces des logiciels malveillants de CopyKittens dans plusieurs attaques ayant visé des sites aussi stratégiques que le Parlement allemand, le ministère turc des Affaires étrangères ou le bureau du Premier ministre israélien… Si les virus du groupe ne sont pas encore d'une sophistication folle – d'où leur détection précoce –, l'ampleur du réseau mis en place montre néanmoins les ambitions de Téhéran en matière de cyberguerre.

Pour mener des opérations clandestines, l'Iran peut puiser dans un vivier intarissable de volontaires. Les bassidjis, le corps de miliciens volontaires supplétif des pasdarans, disposent depuis quelques années d'une branche cyber, même si celle-ci est plus occupée, selon nos informations, à mener des opérations de propagande classique et à traquer les pratiques non musulmanes sur Internet.

Selon certains enquêteurs, Téhéran n'aurait pas opéré seul dans l'affaire Saudi Cables. Dans un article du *Virus Bulletin Conference* d'octobre 2016, deux chercheurs des bureaux américains de la société de cybersécurité russe Kaspersky, Brian Bartholomew et Juan Andres Guerrero-Saade, pointent un autre commanditaire possible de l'opération Saudi Cables : le groupe de hackers russes Fancy Bear… Encore eux !

À l'appui de leur théorie, les deux informaticiens de Kaspersky citent des indices électroniques, notamment des programmes développés par le groupe qu'ils ont retrouvés dans l'intrusion menée sur les messageries saoudiennes. Ils ont même pu établir que Fancy Bear avait identifié début 2015, soit peu de temps avant le vol des données des diplomates saoudiens, une faille dans les réseaux informatiques de la représentation de Riyad à Kiev, faille qui aurait pu permettre aux cybercambrioleurs d'opérer. En outre, les télégrammes saoudiens ont d'abord été publiés sur un site fantôme, wikisaleaks.com, dont l'immatriculation et les adresses IP renvoyaient vers des serveurs basés en Russie. La Yemen Cyber Army pourrait donc n'être qu'un nouvel avatar de Fancy Bear.

Car Moscou, tout comme Téhéran, avait également des raisons d'en vouloir à Riyad en juin 2015. Ennemis traditionnels sur la scène régionale, les deux pays s'affrontent par milices interposées en Syrie : le Kremlin

soutient à bout de bras le régime de Bachar al-Assad, tandis que Riyad finance l'opposition armée sunnite. Le début de l'année 2015 a également été perturbé par une vaste guerre des prix pétroliers, que l'Arabie saoudite a fait plonger. En ne voulant pas diminuer son volume de production, Riyad essouffle les finances publiques russes, à la grande fureur de Vladimir Poutine, engagé militairement sur plusieurs fronts (Syrie, Ukraine).

La fuite des télégrammes diplomatiques saoudiens, qu'elle ait été opérée par l'Iran seul ou avec l'aide d'affidés de la Russie, montre en tout cas qu'un État peut, par le biais d'une simple fuite massive de données sur Internet, déstabiliser profondément un pays ennemi sur la scène internationale. Mieux : impossible à attribuer formellement, ce type d'opérations permet également de tacler secrètement des pays avec lesquels on entretient officiellement des relations cordiales…

*

Le 5 juin 2017, l'Arabie saoudite, les Émirats arabes unis, Bahreïn et l'Égypte décident de concert d'imposer un embargo sur le petit émirat du Qatar. Les quatre pays reprochent à la petite péninsule gorgée de gaz naturel d'être trop proche des Frères musulmans, bêtes noires des régimes autocratiques et dynastiques de la région, mais aussi de l'Iran, l'ennemi stratégique des pays sunnites du Golfe. Les quatre monarchies liguées veulent mettre au pas ce turbulent voisin et tuer dans l'œuf les efforts de Doha pour s'imposer sur la scène régionale.

Le prétexte à la crise est tout trouvé : quelques jours auparavant, l'émir du Qatar, Thamim ben Hamad Al Thani, a lâché plusieurs bombes dans une déclaration à l'agence de presse officielle de son pays, la Qatar News Agency. Il y reconnaît le Hamas, l'organisation islamiste au pouvoir à Gaza, comme « le représentant légitime du peuple palestinien », revendique des « relations fortes » avec l'Iran tout comme avec les États-Unis, et déclare que Téhéran est « une grande puissance de stabilisation de la région ». C'est la stupeur dans les chancelleries occidentales et la colère dans les palais du Golfe.

Sauf que le Qatar, une fois mis au ban par ses voisins, nie énergiquement que son émir ait pu tenir de tels propos et hurle aussitôt au piratage. Selon lui, l'agence de presse du pays aurait été infiltrée par des hackers et la

déclaration de l'émir clandestinement insérée dans le fil des dépêches. Cette explication, qui n'intervient qu'après l'imposition de l'embargo contre le pays, semble bien tardive et particulièrement alambiquée, et laisse les observateurs dubitatifs. Mais Doha s'obstine et, à l'appui de ses dires, fait très officiellement appel aux espions américains de la CIA et du FBI pour enquêter sur l'épisode et, s'il y a effectivement eu piratage, tenter de remonter jusqu'à son origine.

Le *Washington Post* annonce le 16 juillet les résultats de l'enquête américaine : la Qatar News Agency a bien été hackée ! Mieux : les pirates agissaient non pour le compte de la Russie, ni même de l'Iran, mais… pour les Émirats arabes unis, le rival local. Grâce à leur capacité d'interception, les espions américains ont même établi que, le 23 mai, des membres de l'exécutif émirati avaient discuté des préparatifs de l'opération de piratage de l'agence de presse qatarie. Dans un scénario digne des meilleurs romans d'espionnage, ce seraient donc les Émirats arabes unis, dirigés *de facto* par Mohamed ben Zayed Al Nahyan, qui ont eux-mêmes orchestré la « provocation » qatarie qui a suscité la réprobation des pays du Golfe, Émirats en tête !

Certains hauts responsables américains interrogés par le *Washington Post* évoquent ouvertement la possibilité que les Émirats aient sous-traité le piratage de l'agence de presse qatarie à un opérateur privé. Un scénario que nous avons pu confirmer par nos propres sources aux Émirats. Bien qu'ils disposent d'outils de plus en plus performants, les informaticiens de la National Electronic Security Authority (NESA), l'agence de cyberrenseignement locale, n'ont pas – encore ? – les moyens de mener à bien une intrusion aussi sophistiquée.

Comme l'un de nous l'a révélé dans notre publication Intelligence Online, pour remédier à cette faiblesse, la NESA s'appuie depuis quelques mois sur la société américano-israélienne Verint. Celle-ci a remporté un large contrat, d'un montant de cent cinquante millions de dollars, pour mener les interceptions tactiques de l'émirat. Détail piquant : la NESA ne veut pas de hackers originaires de pays arabes pour opérer, mais seulement des citoyens européens ou américains. Décidément, la méfiance règne entre Abu Dhabi et ses amis…

Accusés d'être des agents provocateurs, les Émiratis se défendent en indiquant qu'ils n'ont agi qu'en représailles. Et effectivement, plusieurs

semaines avant le piratage de l'agence de presse qatarie et l'explosion de la crise régionale, un événement a été passé sous silence par Abu Dhabi : des intrus ont pénétré dans la messagerie privée du très influent Youssef Al Otaiba, l'ambassadeur émirati à Washington. Abu Dhabi avait gardé cette intrusion secrète, de peur de passer pour négligent en matière de sécurité informatique. Mais, lorsque les Émirats se sont retrouvés accusés d'avoir piraté l'agence de presse qatarie, le pays n'a eu d'autre choix que de révéler l'agression informatique dont son ambassadeur avait été victime, et dont il attribue la paternité au Qatar…

À peine identifiés, les pirates de la messagerie du diplomate émirati, qui se font appeler GlobalLeaks, ont disséminé leur butin sur la Toile et auprès de nombreux journalistes en vue à Washington. Les mails dérobés exposent la vaste campagne d'influence menée par les Émirats aux États-Unis : lutte contre les Frères musulmans, barrage à l'influence de l'Iran en Occident et, surtout, diabolisation du Qatar…

Le groupe GlobalLeaks, assez mystérieux, a assuré aux médias contactés, dont le journal américain en ligne Daily Beast, qu'il n'avait pas piraté la messagerie de l'ambassadeur émirati, mais avait obtenu les documents auprès d'un « lanceur d'alerte rémunéré », une contradiction dans les termes… GlobalLeaks utilise des adresses mails en « .ru », suggérant que ses membres sont implantés en Russie. Mais tous les cyberexperts que nous avons consultés attribuent l'opération au Qatar. Ils pointent notamment le fait que c'est le site d'actualité Middle East Eye, très proche de Doha, qui publie régulièrement des extraits de la messagerie piratée de l'ambassadeur Al Otaiba. Pour accéder aux messages du diplomate, le Qatar aurait, comme ses adversaires émiratis, sous-traité l'effraction à des hackers privés. Le Golfe fait figure de véritable eldorado pour les cybermercenaires.

L'une de nos sources dans la région, très introduite dans les milieux du renseignement locaux, s'amuse lorsque nous l'interrogeons sur l'épisode GlobalLeaks, qu'elle qualifie de « bisbilles par hackers interposés ». Selon elle, le Qatar et les Émirats ont financé d'autres piratages de ce type, tous menés par des opérateurs privés spécialisés. Certains ont abouti à des déstabilisations publiques, d'autres – et pas des moindres – n'ont jamais été découverts.

*

Selon le renseignement américain, la Corée du Nord s'est également essayée à mener des opérations de *hacking-and-leaking*. Le petit État paria d'Asie, toujours prêt à provoquer l'Occident militairement, serait ainsi à l'origine d'une fuite massive unique en son genre, tant par sa violence que par ses modalités. Elle a été accompagnée d'une opération de chantage, elle aussi massive, et aurait pu entraîner la destruction de tout le système informatique de sa cible, le studio de cinéma Sony !

Le 24 novembre 2014, un groupe de hackers se nommant Guardians of Peace commence à diffuser sur Internet, *via* un forum très fréquenté, Reddit, des documents internes au géant du divertissement Sony. Cette opération a un but bien précis : mettre à genoux l'entreprise. Les pirates affirment en effet avoir infiltré des virus dans les serveurs de la société et réclament, *via* des messages envoyés anonymement aux cadres du groupe, une « compensation financière » si l'entreprise ne veut pas voir ses données éparpillées aux quatre vents.

Plus surprenant, les mal nommés Guardians of Peace menacent également de détruire tout le système informatique de la société grâce aux accès qu'ils se sont ménagés dans le réseau de Sony. Le piratage se double donc d'une véritable opération militaire.

Très rapidement, la piste nord-coréenne commence à être envisagée par les cyberenquêteurs en charge de l'affaire. Leur hypothèse se renforce le 8 décembre lorsque les mystérieux Guardians of Peace demandent en plus de leur « compensation financière » l'annulation de la sortie d'un film de Sony, *The Interview*. Mettant en scène deux stars de Hollywood, Seth Rogen et James Franco, cette comédie raconte comment la CIA monte un complot pour assassiner le leader nord-coréen Kim Jung-un.

Ces premiers éléments de contexte, combinés à l'analyse des logiciels mis en place par le groupe, renforcent la piste nord-coréenne. D'habitude prudente dans ses déclarations sur les piratages, la Maison-Blanche, à la suite du renseignement américain, monte au front et accuse nommément la Corée du Nord d'être à l'origine de l'offensive électronique sur Sony. Pyongyang nie vigoureusement, mais un porte-parole du régime déclare cependant que l'opération pourrait avoir été « un acte de justice perpétré par des soutiens et des sympathisants » du régime. On a vu des dénégations plus virulentes.

La première tempête médiatique passée, les cyberenquêteurs poursuivent leurs investigations. Dépêchés chez Sony, les analystes de la NSA, du FBI et de la société de cybersécurité FireEye découvrent que les pirates sont présents dans les réseaux de Sony depuis plusieurs mois et ont programmé leur attaque en silence. Au total, ils auraient dérobé plusieurs milliers de giga-octets d'informations.

Examinant les cyberoutils laissés derrière eux par les intrus, et reconstituant leurs techniques d'effraction, les experts américains en cybersécurité mobilisés sur ce dossier, privés comme publics, tombent bientôt sur la piste d'une équipe de hackers bien identifiée, le Lazarus Group. Celui-ci a déjà mené des opérations d'envergure, notamment des cyberattaques contre des intérêts sud-coréens. Le premier fait d'armes de ces pirates reste l'intrusion effectuée, *via* l'un de ses logiciels malveillants, dans les réseaux du gouvernement de Séoul, en 2007. Deux ans plus tard, perfectionnant sa technique et ses virus informatiques, Lazarus a mené une série d'attaques massives par déni de service visant là encore plusieurs systèmes informatiques des autorités sud-coréennes. L'attaque par déni de service consiste à bombarder de demandes des serveurs, qui finissent par se mettre hors service. Si le *modus operandi* n'est pas très compliqué, il peut cependant entraîner de sérieux dommages, les serveurs ciblés se retrouvant *in fine* hors réseau. S'il s'agit d'infrastructures critiques – banques, hôpitaux, etc. –, les conséquences peuvent se révéler désastreuses. Le Lazarus Group a lancé ce type d'attaque contre des cibles sud-coréennes jusqu'en 2013, au moins. Selon le FBI et le Département de la sécurité intérieure, le groupe entretiendrait une flotte gigantesque de *botnets*, ces ordinateurs infectés à leur insu, partout dans le monde, pour relayer ses cyberattaques.

Plus récemment, une branche du groupe Lazarus, que la société de cybersécurité Kaspersky, qui l'a découverte, a nommée « Bluenoroff », s'est lancée dans des cyberopérations à visée uniquement financière (attaques de banques, etc.). Ce sont eux, notamment, qui auraient dévalisé plusieurs établissements financiers en pénétrant le système de la Banque centrale du Bangladesh, en 2016. Une autre société, Symantec, soupçonne d'ailleurs Lazarus d'être à l'origine du logiciel malveillant WannaCry, qui a bloqué contre rançon des centaines de milliers d'ordinateurs dans le monde, début 2017.

À l’instar de la menace nucléaire qu’elle fait peser sur la planète, la Corée du Nord dispose en effet d’une vraie capacité de nuisance dans le cyberespace. Pyongyang entretient en particulier une unité dévolue au cyberrenseignement, l’unité 810, rattachée au Bureau général de reconnaissance (BGR), le service de renseignement extérieur. Selon plusieurs transfuges de ce pays, cette unité est à l’origine de nombreuses cyberattaques sur des banques d’Asie du Sud (Philippines, Vietnam, etc.), des opérations menées pour récupérer des devises, dont manque cruellement Pyongyang. Le réseau Internet étant virtuellement inexistant en Corée du Nord, les hackers du BGR se rendraient souvent à l’étranger, notamment en Chine, pour mener leurs opérations.

L’avantage majeur de la Corée du Nord dans le cyberespace, c’est que le pays est à l’abri des représailles : il n’est que très peu relié à Internet, et ses propres réseaux informatiques sont fondés sur des protocoles différents de ceux du reste du monde, donc quasiment hermétiques à toute pénétration.

L’attaque de Lazarus aura été dévastatrice pour Sony. Abondamment repris par la presse, notamment cinéphilique, les documents dérobés sur les réseaux de l’entreprise révèlent le quotidien de Hollywood dans ce qu’il a de moins glorieux : commentaires assassins, complots mesquins, petites et grandes manœuvres entre pontes du cinéma. La présidente de Sony, Amy Pascal, sera ainsi contrainte de démissionner en février 2015, après la divulgation de certains de ses e-mails, jugés racistes. En avril 2015, WikiLeaks publie finalement un large éventail des documents volés par les Guardians of Peace, en justifiant leur publication par « l’aperçu rare du fonctionnement d’une firme multinationale secrète » qu’ils présentent.

Pour ce qui nous occupe dans cet ouvrage, l’aspect le plus intéressant de la fuite massive qui a visé Sony reste la réaction des services américains de renseignement. Dès le départ, ceux-ci ont publiquement identifié l’origine nord-coréenne de l’attaque, pour des raisons tant techniques que politiques. Or attribuer une cyberattaque, surtout à un État, relève toujours d’une volonté de politiser un incident, tant la certitude, en la matière, est difficile à établir techniquement.

Ciblée par de nombreuses fuites massives, l’administration américaine n’hésite plus à attribuer ces incidents à un pays, même si la chaîne de responsabilité est discontinue et les indices informatiques parfois ténus. Les pays européens sont plus prudents, jugeant que la marge d’incertitude

propre aux enquêtes informatiques rend l'attribution d'une fuite massive hasardeuse. À Washington, les caciques du renseignement rétorquent que cette prudence n'est qu'un aveu de faiblesse, l'Europe ne disposant ni des capacités techniques ni de la puissance politique nécessaires pour accuser publiquement un pays d'interférence électronique…

C'est cette prudence qui explique en partie la réticence des autorités françaises à attribuer la cyberattaque qui a visé l'équipe du futur président de la République, Emmanuel Macron, à un opérateur étatique ou à un réseau d'activistes.

*

5 mai 2017. Quarante-huit heures avant le second tour de l'élection présidentielle française, qui oppose Emmanuel Macron à Marine Le Pen, un dossier est anonymement mis en ligne sur le forum américain 4Chan. À l'intérieur, les messages privés de cinq des responsables de la campagne de Macron, favori du scrutin. Quelques jours auparavant, au cours d'un débat télévisé, Marine Le Pen avait menacé son adversaire, déclarant dans un demi-sourire : « J'espère que l'on ne découvrira rien sur vous dans les prochains jours. »

À la veille du vote, les médias français restent muets sur cette fuite : la loi électorale leur interdit tout article susceptible d'influencer le scrutin. Mais cette législation ne concerne que la presse ; très vite, le lien vers les documents est diffusé par le compte Twitter de WikiLeaks, et l'affaire se répand comme un feu de forêt. Une fois Emmanuel Macron élu, les médias français et internationaux s'interrogent : faut-il publier les mails piratés ? Comme pour d'autres fuites ayant visé des candidats politiques, aucun des documents révélés n'est porteur de véritable scandale. Tous montrent le fonctionnement quotidien d'une campagne, en l'occurrence celle du parti de Macron, En marche ! Mais le mode de publication des mails piratés a perturbé les observateurs : la diffusion est en effet intervenue deux jours avant le dimanche de l'élection, au moment où personne ne pouvait réagir, et par un canal inhabituel, 4Chan, un forum assidûment fréquenté par l'extrême droite américaine.

L’hypothèse d’une opération russe est rapidement évoquée : contrairement à Marine Le Pen, qui loue Vladimir Poutine et finance sa campagne grâce à des banques russes, Macron prône la fermeté diplomatique envers Moscou et dénonce le repli populiste. Sur Twitter, la fuite est tout de suite qualifiée de « Macronleaks » et relayée par de faux profils automatiques, dont beaucoup ont été créés en Russie. En avril 2017, l’entreprise japonaise de cybersécurité Trend Micro avait même affirmé dans un rapport que le groupe de hackers russes Fancy Bear tentait de pénétrer les serveurs du parti d’Emmanuel Macron. De son exil londonien, Julian Assange, le fondateur de WikiLeaks, avait également déclaré pendant la campagne que les documents de la messagerie de Hillary Clinton, que le site détenait, révélaient des informations dérangeantes pour Emmanuel Macron, sans que rien ne soit finalement venu corroborer cette assertion. Enfin, les services français de renseignement, ainsi que leurs alliés, États-Unis en tête, multipliaient depuis plusieurs semaines les mises en garde sur une possible ingérence russe dans la campagne électorale française.

D’autres indices, plus probants, convergent eux aussi vers des complicités russes : certains mails piratés ont visiblement été manipulés par des russophones, car les paramètres des documents contiennent des informations en alphabet cyrillique. L’un des messages, écrit par Cédric O., le trésorier de campagne d’Emmanuel Macron, a été modifié par un ingénieur russe, Georgy Petrovitch Rochka. Selon le journal indépendant russe *The Insider*, qui a déchiffré les métadonnées, Rochka est un spécialiste de cryptographie qui a servi dans les unités électroniques de l’armée russe. Or celles-ci sont placées sous la tutelle du GRU, le service de renseignement militaire qui est également le protecteur et, bien souvent, le commanditaire des hackers « patriotiques » de Fancy Bear. Aujourd’hui, Rochka est employé par une société russe de cybersécurité qui a pignon sur rue, Eureka. L’entreprise travaille notamment pour le ministère russe de la Défense, celui des Affaires étrangères ou encore celui de l’Économie, et dispose d’une licence du FSB, le service de renseignement intérieur, pour opérer sur des programmes ayant trait à la sécurité nationale.

Intrigués, comme d’autres, par cette découverte, nous décidons de solliciter l’avis d’un de nos vieux et précieux contacts aux États-Unis : un

ancien officier du GRU, justement, qui s’est reconverti il y a plusieurs années dans le renseignement privé. Et ce, tout en conservant ses relais dans l’appareil d’État russe. Interrogé sur Eureka, il nous transmet une note détaillant le profil de la société. Fondée en 1990, celle-ci est détenue et reste dirigée par trois ingénieurs en informatique : Alexei Nikolaev, Alexander Kinal et Erikh Kotelkov. Elle est spécialisée dans la cybersécurité et dispose également d’un centre destiné à la recherche en failles informatiques. Mais, toujours selon l’enquête de notre contact, Eureka n’est pas l’un de ces sous-traitants auxquels les services de renseignement russes passent commande d’une attaque informatique. Rochka, en revanche, apparaît bien comme un expert en cryptologie : aurait-il pu s’impliquer dans le Macronleaks seul, ou en association avec un groupe de hackers ?

Faute d’indications supplémentaires sur le rôle de ce consultant russe, la piste d’une participation des services du Kremlin dans les Macronleaks se transforme rapidement en impasse. L’amateurisme de l’attaque – une opération de hameçonnage basique – tout comme la diffusion – brouillonne – des e-mails piratés contrastent avec le professionnalisme avec lequel les hackers russes de Fancy Bear orchestrent leurs fuites massives. La publication des messageries piratées du Parti démocrate, par exemple, a été préparée pendant des mois et minutieusement relayée par plusieurs sites. Ce que Guillaume Poupard, le patron de l’Agence nationale de la sécurité des systèmes d’information (Anssi), en charge de l’enquête, a confirmé début juin dans un entretien à l’agence de presse américaine Associated Press (AP), en indiquant que « l’enquête de l’Anssi n’a pas trouvé de trace, derrière le piratage de Macron, du fameux groupe de hackers APT28 », autre pseudonyme de Fancy Bear. Et d’enfoncer le clou : « Sur la base des éléments techniques, qui sont des éléments trop simples, il n’est pas possible de dire “C’est forcément un État” ou “C’est manifestement un groupe criminel”. » Selon Poupard, « ça peut vraiment être n’importe qui, ça pourrait même être un individu isolé. La simplicité technique fait qu’on peut imaginer que ce soit une personne seule qui ait fait ça ».

Et si les serveurs du parti d’Emmanuel Macron, à rebours des professions de foi de son équipe, étaient tout simplement mal protégés ? C’est en tout cas ce que pensent plusieurs autres experts en cybersécurité interrogés par nos soins. Selon eux, les failles des messageries de l’équipe Macron étaient béantes et ne présentaient nulle difficulté pour un pirate, même débutant.

Pas besoin de mobiliser des hackers russes pour pirater les messages des conseillers du candidat.

Une autre piste, celle de militants d'extrême droite américains, semble plus probante : les e-mails volés ont d'abord filtré sur leurs forums. Les services français de renseignement ont d'ailleurs demandé, au printemps, l'aide de leurs homologues américains pour tenter d'y voir plus clair. Une enquête judiciaire a été ouverte début mai et confiée au parquet de Paris, qui dispose d'une section cybercriminalité, dirigée depuis 2015 par la vice-procureure Alice Cherif. Mais, à l'heure où nous écrivons, les cyberenquêteurs français n'ont toujours aucune certitude sur les auteurs du piratage.

Mieux : certains de nos contacts spécialisés dans la surveillance des forums de hackers sur le Darknet ont été surpris que ce soient les messageries d'En marche ! qui aient été piratées. Durant la campagne, ils avaient plutôt repéré des tentatives de pénétration dans les réseaux informatiques de l'adversaire de Macron, la présidente du Front national Marine Le Pen…

Qu'il ait été perpétré par des activistes d'extrême droite ou des hackers téléguidés par la Russie, le piratage des messageries du parti En marche ! d'Emmanuel Macron était avant tout une opération de déstabilisation politique. Les fuites massives sont en effet de plus en plus utilisées pour affaiblir un pays ou un homme politique que pour révéler des informations véritablement cruciales. Signe que les États, à l'origine victime des fuites massives, ont fini par se saisir de cette arme, d'autant plus pratique qu'elle permet d'opérer à couvert et d'infliger des dégâts considérables à peu de frais. À Moscou, à Washington, comme dans le golfe Persique, les batailles géopolitiques se conduisent désormais à coup de mails et de sites Internet anonymes. Mais les États, Russie en tête, ne sont pas les seuls à avoir compris les bénéfices de la fuite massive : le secteur privé, à leur suite, s'est lancé avec enthousiasme dans la subversion par la diffusion d'informations confidentielles. Les entreprises utilisent cette technique pour éliminer des concurrents, gagner des appels d'offres et étayer des procès. Le vol et la diffusion de données par les multinationales constitue, sans doute, l'aspect le plus méconnu du phénomène de la fuite massive.

V

Les receleurs

Les États sont loin d'être les seuls à avoir compris comment transformer la technique des fuites massives inventée par les lanceurs d'alerte en arme de guerre. Dans le secteur privé, grands patrons, avocats, directeurs commerciaux et créanciers ont également vite perçu le potentiel de cette technique de déstabilisation massive. Dans les prétoires et en marge des batailles commerciales et financières, les adversaires n'hésitent plus à se jeter à la figure des liasses d'e-mails aux origines mystérieuses, sous le regard médusé des juges et des régulateurs nationaux.

Disposer d'un accès à des données électroniques privées confère à ceux qui les détiennent des pouvoirs inquisitoriaux démesurés : grâce aux fuites massives, savamment orchestrées, les avocats peuvent concurrencer les juges d'instruction, et les négociateurs inverser les rapports de force. Mais comment recycle-t-on des données piratées dans une procédure judiciaire, dans un bras de fer financier ou une bataille commerciale ? Pour exposer les arcanes de ces guerres électroniques privées, nous avons longuement enquêté sur plusieurs cas de fuites massives, certaines obscures, d'autres très médiatisées, jusqu'à remonter aux bras de fer qui les ont motivées et, parfois, jusqu'aux pirates qui les ont perpétrées. Voyage dans le monde feutré des receleurs de giga-octets…

Tandis que ses collègues du *New York Times*, du *Guardian* et de la *Süddeutsche Zeitung* engrangeaient les prix de journalisme grâce aux fuites d'e-mails et de documents électroniques, Jay Solomon, lui, a vu sa carrière ruinée par l'une de ces fuites. Le 21 juin 2017, il a été brutalement licencié par le *Wall Street Journal*, où il couvrait depuis vingt-trois ans les intrigues politiques du Moyen-Orient. En cause : un dossier de 65 giga-octets contenant huit années d'e-mails et de SMS envoyés par un courtier

américain en avions militaires, Farhad Azima. Dans ce dossier, publié en septembre 2016 sur un réseau *peer-to-peer*, c'est-à-dire accessible seulement aux personnes disposant d'un logiciel commun (les « pairs »), on trouve de nombreux échanges entre Solomon et Farhad Azima. Parmi ceux-ci, une offre commerciale de surveillance aérienne transmise le 16 avril par le journaliste à des responsables des Émirats arabes unis pour le compte d'Azima. En échange de ses services, le reporter du *Wall Street Journal* s'était vu offrir 10 % dans l'une des sociétés d'Azima. Horrifié par ce mélange des genres, le *Wall Street Journal* s'est séparé de son reporter séance tenante.

Mais les mails d'Azima ne gênent pas le seul *Wall Street Journal* : né en Iran, Farhad Azima entretient des relations suivies avec de très nombreux journalistes et a l'habitude d'organiser chaque année des cocktails en marge de l'Assemblée générale des Nations unies à New York. S'y retrouvent tous les correspondants des principaux journaux américains. Sa messagerie est truffée d'échanges avec les spécialistes en politique étrangère des grands médias, dont il était une source fidèle. Et pour cause ! Derrière son image de courtier, Farhad Azima est en réalité un sous-traitant régulier de la CIA, pour laquelle il a longtemps transporté des cargaisons d'armes légères, notamment en Iran, au Nicaragua et en Croatie. Ses avions ont également acheminé des soldats américains en Irak, ainsi que des ravitaillements pour le contingent de l'OTAN en Afghanistan.

Contre toute attente, ce ne sont pas ses missions clandestines qui ont valu à Farhad Azima de voir sa messagerie piratée et diffusée sur Internet : c'est un banal conflit commercial. Car, après les espions, les avocats ont à leur tour compris tous les avantages du hacking et n'hésitent plus, pour faire avancer leurs dossiers, à introduire devant les tribunaux ou les cours d'arbitrage des messages vraisemblablement piratés. Rencontré dans les bureaux immaculés du cabinet d'investigation américain Kroll, spécialiste des enquêtes délicates pour le compte des entreprises, un ex-procureur qui a quitté les prétoires pour devenir consultant privé nous a longuement expliqué comment on peut étoffer une plainte pénale avec des e-mails issus d'un piratage : « Supposons que je me trouve en possession d'une copie de votre messagerie privée, et que je sache qu'elle a été dupliquée sans votre consentement… » (Mais pourquoi donc tous nos interlocuteurs prennent-ils systématiquement cet exemple pour étayer leurs démonstrations devant nous qui vivons, depuis le début de cette enquête, dans la crainte de voir

nos boîtes mails piratées ?) « Supposons également que votre correspondance électronique prouve que vous avez commis un délit à mon encontre. Si j'utilise vos e-mails pour déposer une plainte, il faudra que j'explique au juge comment je les ai obtenus ; et cela risque d'être difficile… » Dans le monde anglo-saxon, en effet, les juges d'instruction n'existent pas : le rôle des magistrats n'est pas d'enquêter, mais d'arbitrer entre les parties. Ce sont donc les plaignants qui doivent étayer leurs accusations – c'est la raison pour laquelle ils utilisent des enquêteurs privés. En conséquence, ils sont tenus d'expliquer comment ils ont obtenu les preuves qui confirment leurs dires. S'ils soumettent à un juge des pièces dont ils ne peuvent expliquer l'origine, ils risquent de passer très vite du banc des plaignants à celui des accusés. C'est la raison pour laquelle tous les avocats prennent bien soin de ne s'appuyer que sur des piratages qui ont été diffusés au préalable sur Internet : leur provenance est facile à expliquer, et les juges ne peuvent les écarter sans les avoir examinés. « En contre-interrogatoire ou en réponse, en revanche, il est beaucoup plus facile d'exhiber un document, même piraté, pour montrer que votre adversaire ment. Les juges n'aiment pas le mensonge et s'inquiéteront d'abord de savoir si la pièce est authentique avant de vous demander comment vous l'avez obtenue. Si jamais ils le font. » En cour d'arbitrage, les juges sont privés et les auditions confidentielles : les critères d'évaluation des preuves sont encore plus flous et tous les moyens sont bons…

Autour d'une bière, dans un pub de Mayfair, deux vétérans du *litigation support*, un euphémisme qui désigne les détectives travaillant pour des avocats, nous ont décrit une autre méthode pour introduire des e-mails piratés dans une procédure. « Tout cela est bien évidemment hypothétique ! nous assurent-ils avec un sourire gourmand. Le fait que l'on sache comment procéder ne veut bien évidemment pas dire qu'on l'a déjà fait. » Pas vu pas pris : nous commençons à connaître le refrain… « En fait, c'est assez simple : supposons qu'un avocat ait récupéré des messages particulièrement compromettants échangés par des parties avec lesquelles il est en procès. S'il s'agit d'un dossier international, comme le sont la quasi-totalité des affaires sur lesquelles nous travaillons, il va s'arranger pour présenter ces e-mails non pas à une juridiction européenne ou américaine, qui, immanquablement, lui demanderait comment il les a obtenus, mais devant une cour plus exotique, par exemple à Bahreïn, ou aux Émirats arabes unis,

où les normes en matière d'obtention de preuve sont moins élevées. Ensuite, une fois que ces documents piratés ont été blanchis par des juges au Moyen-Orient ou ailleurs, l'avocat dépose plainte en Europe ou aux États-Unis et joint à cette plainte la procédure étrangère, qui contient les mails. Et voilà, le tour est joué ! »

Ce récit, on s'en doute, n'a rien d'hypothétique : on retrouve la manœuvre dans plusieurs procès financiers dans le golfe Persique, notamment dans la bataille judiciaire qui oppose Ras al-Khayma, l'un des sept territoires qui composent les Émirats arabes unis, au financier suisso-libanais Khater Massaad, qui fut pendant cinq ans chargé de faire fructifier l'épargne nationale. En 2012, le petit émirat licencie Massaad et l'accuse d'avoir détourné à son profit près d'1,5 milliard de dollars de fonds publics. L'ex-banquier aurait réalisé une série d'investissements, notamment en Géorgie, à des prix surévalués, et empoché la différence grâce à des complices. Nombre de procès sont initiés, aux Émirats, mais également à Londres et en Suisse. Aucune de ces procédures ne permet d'établir nettement la culpabilité de Khater Massaad. Or ce préalable est indispensable si l'émirat veut récupérer l'argent détourné.

Ne parvenant pas à ses fins, l'émirat change brusquement de tactique. À l'été 2016, les boîtes mails de Khater Massaad et de plusieurs de ses proches sont piratées. Le contenu des messages est rapidement soumis au tribunal de Ras al-Khayma chargé de juger l'affaire et, par ricochet, atterrit miraculeusement devant les tribunaux britanniques et suisses également saisis du dossier. Les mails hackés sont transmis à l'Arabie saoudite, où Khater Massaad s'est réfugié. Sur la base de ces informations, qui n'ont jamais été rendues publiques, il est rapidement arrêté et placé en résidence surveillée.

La cyberoffensive s'étend à tout l'entourage du financier déchu. Proche de Khater Massaad et associé à lui sur une opération en Géorgie, Farhad Azima, le transporteur aérien de la CIA, voit également sa messagerie attaquée et jointe à la procédure. Pour lui, le coup est dévastateur : opérant dans l'ombre, toute publicité lui est mortelle. L'homme d'affaires a déjà été éclaboussé par une autre fuite massive, celle des Panama Papers, qui a révélé qu'il gérait une collection de sociétés offshore au Panama. Mais la perte de sa messagerie personnelle est autrement plus dommageable. Pour

tenter de se défendre, Farhad Azima se tourne à son tour vers les tribunaux et porte plainte contre Ras al-Khayma pour piratage. Durant les auditions, l'émirat se défend de toute action illégale et évoque même la possibilité que l'intrusion dans la messagerie de l'homme d'affaires ait été commanditée… par la Russie, Farhad Azima étant l'un des donateurs de la fondation de Bill Clinton, dont la campagne présidentielle de la femme a été ciblée quelques mois plus tôt par des attaques informatiques attribuées à Moscou.

Farhad Azima réclame 20 millions de dollars à Ras al-Khayma et tente d'obtenir la mise sous scellés de ses e-mails piratés. Peine perdue : sur la foi de ces messages, exposés au tribunal, le département américain de la Justice ouvre une enquête sur ses activités en Géorgie et sur ses partenaires iraniens. Pire : le 20 juin 2017, trois journalistes d'Associated Press publient une longue enquête fondée sur un examen minutieux de ses e-mails. On découvre alors que Farhad Azima possède une société avec deux anciens agents de la CIA, et que les trois hommes ont prêté main-forte à un héritier de la couronne koweïtienne qui cherchait à prendre le pouvoir. Azima et ses associés ont également tenté de vendre des services de surveillance aérienne aux Émirats arabes unis (c'est dans cette opération que le journaliste du *Wall Street Journal*, Jay Solomon, est intervenu comme intermédiaire).

Après cette habile utilisation de sa propre messagerie à son encontre, le courtier favori de la CIA n'a plus qu'à mettre la clef sous la porte. C'est un *modus operandi* que nous retrouverons régulièrement tout au long de nos enquêtes : plus un homme d'affaires recherche la discrétion, plus il est vulnérable à une exposition de ses communications. Si ses activités, comme c'est le cas pour Farhad Azima, sont couvertes par le secret-défense, la simple menace d'une divulgation de sa messagerie équivaut à une intimidation nucléaire.

*

Dans cette cyberguérilla mondiale, les avocats et les conseils juridiques sont en première ligne : ce sont eux qui sont les plus exposés à des tentatives de piratage, soit pour décrédibiliser leur client, soit pour nourrir la plainte de la partie adverse. Pour prévenir de tels incidents, qui peuvent faire chavirer une procédure, tous les grands cabinets d'avocats mondiaux

se sont donc dotés de départements informatiques conséquents pour protéger leurs réseaux, mais également enquêter sur les offensives dont ils sont victimes. Voire pour lancer eux-mêmes des piratages ? À cette question faussement naïve, deux de nos interlocuteurs, très introduits dans la communauté juridique suisse, manquent de lâcher leur fourchette : « Vous êtes fous ! Aucun avocat ne fera un hacking à partir de ses propres réseaux ! Cela reviendrait à signer l'opération ! »

Dans ce restaurant familial qui domine l'un des plus beaux lacs suisses, entourés de retraités venus profiter de la vue, nous jouons les ingénus en reprenant généreusement du gâteau au chocolat suisse sur le chariot des desserts :

– Mais si les avocats n'opèrent pas eux-mêmes, sur qui se reposent-ils ?

– Eh bien, hypothétiquement [ce mot, toujours !], ils mandatent des hackers avec lesquels ils n'ont aucun lien direct.

– Et ils n'ont pas peur que ces prestataires, d'un genre un peu particulier tout de même, ne se retournent contre eux ?

– Non : tout est très sécurisé. Je vais prendre un exemple : supposons que je veuille commanditer un piratage sur vos messageries à tous les deux [cet exemple, toujours et encore…]. Eh bien, j'irais sur le Darknet, cette partie d'Internet non répertoriée par les moteurs de recherche, et fréquentée, à l'abri des regards indiscrets, par toute la communauté du piratage mondial, mais également par les revendeurs de drogue, d'armes, de pornographie, etc. Je prendrai un pseudonyme et j'irai m'inscrire sur un forum de hackers.

Comment trouve-t-on une de ces listes de discussion puisqu'elles ne sont signalées nulle part ? « Par bouche-à-oreille, à force de fréquenter ce milieu. Bref, une fois inscrit sur le forum, j'exprimerai mon besoin et, si mon annonce trouve preneur, je négocierai un prix et testerai d'abord mon hacker sur un objectif que je maîtrise : une messagerie à laquelle j'ai accès, par exemple, ou bien un compte en banque dont j'ai les codes. Si ce test est satisfaisant, si le pirate parvient à récupérer les données que je lui ai commandées et ne les utilise pas pour son propre compte, et si le paiement se passe bien, je lui donnerai une seconde mission, la vraie, celle-ci, à savoir pirater vos mails. » Tout cela a effectivement l'air très facile, mais,

pour payer le pirate, il est tout de même nécessaire de le rencontrer, non ? « Pas du tout : le règlement s'effectue en bitcoins, cette monnaie virtuelle et cryptée. On dépose les bitcoins sur un compte séquestre électronique et, une fois la mission effectuée, on libère l'argent. C'est très pratique, et ça ne laisse pas de traces. »

Entre la poire et le fromage s'ouvre une fenêtre sur un autre monde. Un monde où les hackers ne sont pas ces légions anonymes lancées à l'assaut du capitalisme, mais bien plutôt des professionnels corvéables et répertoriés, agissant à la commission pour des intérêts qui les dépassent et dont, souvent, ils ignorent tout. Un monde où les multinationales, bien loin d'être assiégées par les bataillons du cyber-*underground*, se sont au contraire merveilleusement acclimatées à la nouvelle donne mondiale et restent aux commandes, même dans les marges électroniques les moins hospitalières.

*

Le système est tellement bien rodé que, de plus en plus, c'est Internet lui-même qui sert de prétoire, les institutions juridiques nationales se trouvant reléguées au rang de chambres d'enregistrement des offensives menées sans frein sur le réseau mondial. Sur Internet, un plaignant peut inverser le rapport de force qui l'oppose à son adversaire en détruisant sa réputation et obtenir l'abandon de procédures judiciaires. C'est ce qui s'est passé en marge des Panama Papers, la fuite massive de documents internes au cabinet panaméen Mossack Fonseca, spécialisé dans l'enregistrement de sociétés offshore. La fuite est orchestrée en avril 2016 par le quotidien allemand *SonntagsZeitung*, associé pour l'occasion au *Monde* et au *Guardian*. L'histoire, telle que l'ont racontée ces journaux, a fait le tour du monde : une source anonyme leur a fourni en direct, et pendant près d'une année, les e-mails et les documents échangés en interne par les employés de Mossack Fonseca. Soit près de 1,5 million de dossiers et 2,6 téraoctets de données. Cette source, baptisée « John Doe », a toujours été identifiée comme un lanceur d'alerte, c'est-à-dire quelqu'un ayant connaissance de malversations dans le cadre de ses activités professionnelles et bravant les règles de non-divulgation de secrets pour les mettre sur la place publique. Autrement dit, un employé ou un sous-traitant de Mossack Fonseca. Mais,

dans un message envoyé à tous ses clients peu après la fuite, Mossack Fonseca raconte une histoire très différente : selon le cabinet, ses serveurs auraient été piratés par un opérateur extérieur, profitant d'une faille dans son serveur de paiement. Une plainte, très peu médiatisée, a même été déposée au Panama pour « piratage ». Mais qui aurait eu intérêt à hacker le système de Mossack Fonseca ? Simple agent fiscal, le cabinet n'avait pas d'ennemi connu, pas de procès répertorié.

Une recherche plus approfondie montre que cette assertion n'est pas tout à fait exacte : au moment même où sa base de données fuite, Mossack Fonseca est engagé depuis plusieurs années dans un violent bras de fer avec l'un des fonds les plus agressifs du monde, Elliott Management. Fondé par le financier Paul Singer, Elliott est une véritable légende à Wall Street : ce fonds ultrasecret s'est spécialisé dans le rachat de dettes, en particulier d'État. La technique d'Elliott, c'est de rafler à bas prix de la dette décotée, et ensuite d'obliger ses débiteurs à payer la totalité de la créance, sans décote. Pour parvenir à ses fins, Elliott harasse ses cibles à coups de procès interminables et n'hésite pas, preuve à l'appui, à les accuser de corruption par médias interposés : le fonds entretient une relation étroite avec les journalistes, qu'il alimente en informations susceptibles d'affaiblir ses adversaires. La République du Congo et le Pérou ont chacun fait les frais de ces tactiques agressives, mais la principale cible d'Elliott depuis 2002, c'est l'Argentine. Le fonds détient 630 millions de bons obligataires argentins et bataille pour que Buenos Aires s'en acquitte en totalité, intérêts compris, ce qui représente 2,3 milliards de dollars en tout. Pour tordre le bras du pays, Elliott n'a pas hésité à mandater des armées de détectives privés pour enquêter sur la fortune de la présidente, Cristina Kirchner, et même faire brièvement saisir des bateaux de guerre argentins qui croisaient au large du Ghana.

Or Mossack Fonseca, le discret agent offshore panaméen, est impliqué, bien malgré lui, dans la guerre entre Elliott et l'Argentine. Le cabinet a immatriculé 123 sociétés offshore qu'Elliott soupçonne d'être liées à la présidente Cristina Kirchner : celle-ci, accuse Elliott, aurait utilisé ces coquilles panaméennes pour détourner de l'argent public argentin. Pour se rembourser de ses créances, Elliott veut saisir ces sociétés et, pour obliger Mossack Fonseca à en déclarer les ayants droit, a initié un vaste procès dans l'État américain du Nevada. Lorsque « John Doe », la mystérieuse source des Panama Papers, commence à transmettre ses fichiers aux journalistes

allemands, le procès entre Mossack et Elliott bat son plein. Or les tout premiers dossiers communiqués par « John Doe » sont précisément… les actes des sociétés argentines qu'Eliott cherche depuis plusieurs années à obtenir devant les tribunaux ! Ces documents ne seront bien évidemment pas les seuls transmis aux journalistes, mais, premiers reçus, ils figureront de manière proéminente dans le feuilleton des Panama Papers, que le quotidien allemand *SonntagsZeitung* commence à publier le 3 avril 2016.

Immédiatement, le scandale est mondial. En Islande et au Royaume-Uni, deux Premiers ministres sont en difficulté à cause de leurs sociétés offshore situées dans le petit pays d'Amérique centrale. Les familles royales espagnole et qatarie sont elles aussi éclaboussées, de même que le Kremlin et, bien sûr, la présidence d'Argentine. Pris dans la tourmente, Mossack et Buenos Aires capitulent très vite. Elliott n'a même pas besoin de présenter aux tribunaux les documents qui viennent d'être révélés sur Internet. Le 13 avril, soit moins de dix jours après le lancement des Panama Papers, l'Argentine négocie un compromis avec le fonds et s'acquitte de sa dette sans barguigner. En un éclair, une fuite massive de documents aura réglé un procès vieux de quinze ans, et ce, sans même qu'il soit nécessaire d'en passer par les instances judiciaires. Le tribunal mondial d'Internet a fait plier les instances nationales.

Elliott est-il à l'origine des Panama Papers ? Hormis une série de coïncidences troublantes, rien ne permet de l'établir. L'ampleur de la fuite, planétaire, dépasse largement les intérêts propres du fonds, même s'il est connu pour ses techniques très agressives et pour sa propension à monter des dossiers sur ses adversaires et à les transmettre aux journalistes. Client fidèle des plus grands cabinets d'enquête privés américains, Elliott est l'un des très rares géants de Wall Street à disposer de son propre service de renseignement, dirigé par un ancien officier britannique. Le fonds a-t-il mandaté des recherches sur les sociétés offshore de la famille présidentielle argentine et s'est-il laissé déborder par son sous-traitant ? Cette théorie, entendue chez nos interlocuteurs évoluant dans le monde de l'information grise, ne peut dépasser le stade de l'hypothèse. Dans le long combat d'ombre qu'est notre enquête, nous avons dû sans cesse nous garder contre les raccourcis faciles et les théories du complot. Cela posé, le cas des Panama Papers montre clairement que les fuites massives ne bénéficient pas

uniquement à la transparence mondiale, mais permettent également à de puissants intérêts financiers de faire avancer leur cause. Nous en aurons confirmation à l'été 2016, quand un détective exhibera devant nous une liasse de documents internes à Mossack Fonseca que les journaux qui ont révélé les Panama Papers n'ont jamais publiés. Comment les a-t-il obtenus ? « Oh, ça circule dans notre milieu… », nous répondra-t-il avec un sourire mystérieux.

*

De plus en plus cantonnés au rôle de chambre d'enregistrement, les tribunaux restent malgré tout l'un des derniers forums où l'origine des fuites massives a une chance d'être exposée. Ces dernières années, les instances judiciaires se sont dotées de procureurs spécialisés dans les enquêtes informatiques : c'est notamment le cas en France, où le parquet de Paris dispose d'une section cybercriminalité, dirigée depuis 2015 par la vice-procureure Alice Cherif. C'est elle qui mène l'enquête sur le piratage des messageries du parti d'Emmanuel Macron, En marche !, et leur diffusion sur le forum 4chan à la veille du second tour de l'élection présidentielle de 2017.

Dans les conflits commerciaux, les juges n'hésitent plus à convoquer à la barre des experts informatiques pour examiner les pièces d'un procès et établir leur éventuelle manipulation. C'est ce qui s'est passé à la High Court de Londres, dans une spectaculaire affaire de fuite massive qui, à la suite du témoignage d'un informaticien, s'est retournée contre le plaignant.

L'affaire concerne le conglomérat saoudien Dar al-Arkan, le plus gros promoteur immobilier du royaume, qui gère un portefeuille de projets de trois milliards de dollars, parmi lesquels des lotissements de luxe à l'architecture « parisienne » en plein désert, des galeries commerciales géantes, des tours de bureaux et d'habitations, et même un complexe hôtelier dans l'enceinte de la mosquée du Prophète, à La Mecque. Le groupe appartient à une famille saoudienne richissime, les Al-Shelash. En août 2010, ceux-ci licencient leur directeur général, Majid al-Refai, et portent plainte contre lui pour détournement d'argent. Quelque temps après cet incident, deux sites, sukuk-compliance.com et daralarkan-crisis.com, font leur apparition sur Internet. Très vite, ils multiplient les révélations sur

le groupe Dar al-Arkan : documents internes à l'appui, on y apprend que la société ne survit que grâce à des transactions factices avec son principal actionnaire, la famille Al-Shelash, et qu'elle est contrôlée *via* deux sociétés offshore, enregistrées dans les îles Caïmans. L'effet de cette fuite est dévastateur : l'agence de notation Standard & Poor's dégrade immédiatement la note de Dar al-Arkan, empêchant l'entreprise d'emprunter sur les marchés internationaux. Pour la famille Al-Shelash, il devient vital de bâillonner les sites qui l'accusent, sous peine de tout perdre. Le groupe soupçonne évidemment le directeur qu'il vient de licencier, mais n'a aucune preuve pour étayer ses soupçons.

Un petit cabinet d'enquête informatique autrichien, Information Security Consulting, est donc appelé à la rescousse. Parmi ses services, la société liste la « lutte contre la diffamation en ligne » et l'« interception de conversations électroniques ». Les consultants autrichiens se mettent au travail et tentent de désactiver les deux sites qui, chaque jour, continuent de publier des documents internes au conglomérat Dar al-Arkan. Pour confondre son ancien employé, le groupe saoudien mandate également des enquêteurs privés afin de retrouver les comptes en banque de Majid al-Refai partout dans le monde (les détectives en identifieront dix-sept). C'est dans cette période de frénésie que, selon la version officielle, deux colis arrivent miraculeusement au siège de Dar al-Arkan, à Riyad. L'adresse est griffonnée à la main, et l'expéditeur est inconnu. À l'intérieur, deux disques durs contenant des milliers d'e-mails issus de la messagerie personnelle de Majid al-Refai, l'ancien directeur général licencié. Ces documents montrent que c'est bien lui qui alimente en documents confidentiels les deux sites qui multiplient les révélations sur son ancien employeur, et qu'il le fait avec l'aide de deux cabinets anglais, la société d'enquête Kroll et l'agence de communication FTI. Sur la base de ces messages, la société Dar al-Arkan porte plainte à Londres contre son ex-dirigeant et ses consultants. Peu de temps après, les deux sites disparaissent.

Victoire ? Pas tout à fait… Car le dossier de Dar al-Arkan s'écroule à la barre, et le groupe, d'accusateur, se retrouve sur le banc des accusés. Les deux disques durs reçus par la poste constituant l'essentiel des preuves du dossier, la justice britannique demande leur expertise. L'examen est confié à l'un des enquêteurs les mieux introduits dans la City, Max Hoskinson,

patron du cabinet d'investigation informatique Grey Heron, qui s'est distingué dans les violentes batailles qui ont opposé plusieurs oligarques installés à Londres. Rapidement, les experts de Grey Heron montrent que les e-mails contenus sur les deux disques ont été piratés, et trouvent même, dans les métadonnées associées aux fichiers électroniques, l'identité du hacker : HaCkOoR, alias Bassam Salman, célèbre pour ses exploits informatiques au Moyen-Orient. Or le pirate est actuellement employé dans une entreprise saoudienne détenue par Ali Saleh al-Othaim, qui s'avère être… un intime de la famille Al-Shelash et un actionnaire de leur entreprise, Dar al-Arkan. Sommé à la barre de la High Court de Londres, l'homme d'affaires saoudien explique qu'effectivement il a demandé à son informaticien de s'intéresser à Majid al-Refai et lui a dans ce but fourni toutes les informations nécessaires, notamment les adresses mails de l'ancien directeur général de Dar al-Arkan sous la forme d'un fichier Excel. Il reconnaît également que, une fois les messageries piratées, il a préféré envoyer les e-mails récupérés de manière anonyme à la société Dar al-Arkan, pour ne pas laisser de traces… Dévastateur, le témoignage fait basculer le procès : le géant saoudien de l'immobilier est immédiatement accusé de dissimulation et de manœuvres malhonnêtes et doit précipitamment battre en retraite.

Arme de déstabilisation massive, la fuite massive peut avoir un effet tout aussi dévastateur pour celui qui l'orchestre, s'il vient à être découvert. Ces « effets de souffle » sont cependant peu nombreux : opérant derrière des paravents de pseudonymes et de serveurs-relais, les cyberreceleurs sont rarement découverts. Et si par malchance ils le sont, ils peuvent toujours se faire passer pour des « lanceurs d'alerte ».

*

Malgré l'ampleur des conflits qui le traversent, souvent éclatés sur trois continents, le cyber-village mondial, on l'a dit, reste minuscule : on y retrouve sans cesse les mêmes personnages qui, alternativement, défendent un camp, puis l'autre, dans les affaires de fuite massive. Ce qui est vrai chez les informaticiens israéliens l'est aussi chez les avocats : derrière les grandes affaires de divulgation de correspondance, on retrouve toujours les

mêmes juristes rompus à la guérilla informatique, les mêmes consultants et, souvent, les mêmes hackers.

Ainsi le cabinet britannique Dechert était-il, au même moment, l'avocat du géant de l'immobilier saoudien Dar al-Arkan, en guerre avec son ancien directeur, et celui de l'émirat de Ras al-Khayma traquant son ancien trésorier, Khater Massaad. Et, dans les deux cas, le client de Dechert a organisé un piratage massif de son adversaire pour l'emporter.

En face, c'est la même chose : Khater Massaad, le gestionnaire déchu de la fortune de Ras al-Khayma, a choisi pour le défendre et contester l'usage judiciaire de sa correspondance les pénalistes genevois de Lalive. Or, la même année, ce même cabinet, spécialisé dans les bras de fer internationaux, a défendu le clan kazakh Krapunov, en guerre contre son gouvernement et victime, lui aussi, de tentative de piratage vraisemblablement organisée par le Kazakhstan…

Cette plasticité s'étend également aux consultants : Grey Heron, le cabinet d'expertise informatique qui a mis au jour le piratage organisé par Dar al-Arkan, le géant de l'immobilier saoudien, est adossé à une autre société, De Facto, spécialisée, elle, dans des opérations nettement plus offensives. Quelques années avant que Grey Heron ne démêle, à la barre du tribunal de Londres, les manœuvres informatiques de Dar al-Arkan, De Facto avait mené des opérations très similaires pour le groupe de transport maritime public russe Sovcomflot, en conflit, là encore, avec d'anciens dirigeants accusés d'escroquerie. Pour confondre les cadres renégats, De Facto avait monté une opération baptisée « Projet Esturgeon », récupéré des numéros de comptes bancaires et surveillé des téléphones portables. Une campagne qui, comme l'affaire Dar al-Arkan, s'était terminée devant la High Court de Londres, mais dont De Facto est sorti largement indemne.

Phénomènes apparemment volatils et aléatoires, les fuites massives de données dans le secteur privé ont été jusqu'à présent gérées par une toute petite communauté très consanguine où tout le monde se connaît et, suivant les dossiers, s'affronte ou s'associe. Ces professionnels du « Leak » restent le plus souvent dans l'ombre et ne sont que très rarement éclaboussés par les procès qu'ils orchestrent en coulisses. Quelquefois, les événements leur échappent, et ils se retrouvent en pleine lumière. C'est ce qui est arrivé en juillet 2015 à la société italienne Hacking Team.

*

Alberto Ornaghi et Marco Valleri ont un sens du marketing indéniable : pirates patentés, ils ont choisi au début des années 2000 de baptiser leur société « Hacking Team ». L'entreprise a été mise sur pied pour commercialiser à la police italienne des outils développés par les deux bidouilleurs informatiques dans leur chambre. Ornaghi et Valleri étaient alors des pirates opérant sous les pseudonymes ALoR et NaGA et avaient inventé un outil, Ettercap, capable de prendre le contrôle d'un ordinateur à distance. Rapidement, la société a développé une gamme de produits qui promettaient d'obtenir le même résultat sur les téléphones mobiles, les tablettes, et tout type d'ordinateur. La société a commencé à les vendre à tous les services de police et de renseignement du monde.

Pour un spécialiste de l'intrusion informatique, la pire chose qui puisse arriver est évidemment d'être infiltré soi-même. Et après dix années de développement tous azimuts, c'est précisément ce qui est arrivé à Hacking Team le 5 juillet 2015. Ce jour-là, un message sur le fil Twitter de la compagnie proclame : « Puisque nous n'avons rien à cacher, nous publions tous nos e-mails, dossiers et codes-sources », soit tout le patrimoine informatique du groupe. Le message est accompagné d'un lien vers un site de *peer-to-peer*, BitTorrent, un système d'échange de données en ligne, très utilisé pour télécharger des films et des fichiers musicaux. Le lien conduit vers un fichier compressé contenant 400 gigaoctets de données internes à Hacking Team. L'effet est dévastateur : en quelques jours, tous les secrets industriels du groupe se trouvent sur la place publique, et notamment les failles informatiques utilisées par les outils de Hacking Team pour pénétrer les ordinateurs. À la lecture de ces informations, tous les géants mondiaux de l'informatique réparent à la hâte les défauts de programmation utilisés par Hacking Team pour subvertir leurs logiciels, rendant certaines des solutions du groupe inopérantes.

Humiliation suprême, « Phineas Fisher », le hacker qui dit avoir pénétré le système de la société, publie un très long texte détaillant comment il a procédé, montrant que les réseaux de Hacking Team sont mal protégés contre des pénétrations externes, alors que le piratage est supposé être la spécialité de la société.

Phineas Fisher justifie son attaque contre Hacking Team au nom de la lutte contre la surveillance d'État. L'année précédente, un pirate portant le même nom avait déjà mené une opération similaire contre un autre sous-traitant, Gamma International, fabricant du logiciel de pénétration informatique FinFisher. S'agit-il de la même personne ? Impossible de savoir : dans le cyber-*underground*, les alias et les pseudonymes s'échangent plus facilement que les masques un jour de carnaval. Officiellement, donc, Hacking Team a été victime de cybercroisés prêts à tout pour défendre les libertés individuelles. Mais les dirigeants de la société, anciens pirates eux-mêmes, sont familiers des acrobaties rhétoriques utilisées par les hackers pour brouiller les pistes et font une tout autre lecture de l'incident. Au moment où ils ont été hackés, ils étaient en procès depuis trois mois avec plusieurs employés qui, tout en continuant à travailler pour eux, avaient développé pour leurs clients personnels une contre-mesure qui… permettait de déjouer les logiciels de piratage développés par leurs employeurs !

Ces outils étaient commercialisés *via* une société américaine, ReaQta, contrôlée en sous-main par un groupe de salariés et de commerciaux de Hacking Team. Informés de la manœuvre, l'entreprise italienne avait mandaté le cabinet d'enquête Kroll pour infiltrer et confondre les employés renégats, puis, sur la base des éléments collectés par les enquêteurs, puis porter plainte à Milan pour concurrence déloyale, mais, surtout, pour vol de secrets industriels : les outils d'antipiratage de ReaQta ne pouvaient qu'avoir été développés à partir des logiciels de Hacking Team, puisque leur principale fonction était d'en bloquer l'usage.

Une offensive judiciaire soigneusement paramétrée, mais balayée par la fuite massive des disques durs de Hacking Team. Après leurs publications, la société italienne s'est elle-même retrouvée devant les tribunaux, ses e-mails révélant qu'elle avait commercé avec des régimes sous sanctions, notamment le Soudan. Affaibli par la divulgation de ses données, le groupe a dû lutter pour sa survie, et le procès intenté à ses employés est mécaniquement passé au second plan. En outre, les secrets industriels de Hacking Team étant désormais disséminés sur Internet et accessibles à tous, il devenait presque impossible de prouver qu'ils avaient été détournés en interne par des salariés indélicats.

Hacking Team a-t-elle été visée par des activistes ou par ses propres salariés ? La question suscite un long silence chez notre interlocuteur, l'un des détectives les plus chevronnés de Washington, qui a longuement travaillé sur cette affaire. Familier des intrigues qui prospèrent à l'ombre du Capitole, l'homme a participé à l'enquête commanditée par la société italienne contre ses salariés. Il a accepté de nous rencontrer au restaurant Old Ebbit Grill, la chambre d'écho des rumeurs de Washington, située juste en face de la Maison-Blanche. Autour de nous, sénateurs, lobbyistes et attachés parlementaires troquent de l'information, matière première de la ville. Notre détective, visiblement mal à l'aise avec l'affaire Hacking Team, tente de détourner la conversation, mais nous revenons sans cesse sur le sujet. Chipotant ses œufs brouillés au bacon, il finit par nous lâcher qu'il n'a pas compris tout ce qui s'était passé dans cette histoire, mais qu'il y a « incontestablement eu des fuites organisées. Par qui et pourquoi, je ne sais pas. J'ai été pris dans l'ouragan et ai vu avec déplaisir mon nom cité dans les mails qui ont été divulgués. J'ai essayé d'en savoir plus, mais n'y suis jamais véritablement parvenu. Je n'ai pas très envie de revenir sur tout ça, pour moi c'est du passé ».

Pour un détective traditionnel comme lui, plus à l'aise dans les couloirs du Congrès que devant une batterie d'ordinateur, les fuites massives de données génèrent-elles de l'activité ? « Je suis rarement mandaté dans ce genre d'affaires : trop technique pour un vieux renard comme moi… Sauf quand les vols de données suscitent des tentatives de chantage et que les déjouer nécessite de s'infiltrer chez l'adversaire. Là, on fait appel à moi. »

Dans le cybervillage, la publication de données volées sur Internet peut en effet solder une tentative d'extorsion ratée. Nombreux sont les individus et les entreprises qui, une fois leurs disques durs piratés, se sont vu proposer de récupérer leurs documents volés contre rançon. En enquêtant, nous nous sommes rendu compte que ces cas sont plus fréquents que l'on n'imagine. Mais personne n'en parle : lorsqu'un échange de données est négocié, les victimes, pas plus que les maîtres chanteurs, n'ont intérêt à l'ébruiter. Les cyber-extorsions ne deviennent des fuites d'informations publiques que lorsqu'elles échouent. C'est ce qui est arrivé au fonds d'investissement maltais Doyen Sport au printemps 2016.

*

Il fait un soleil éclatant sur Pall Mall, la grande artère londonienne qui relie Trafalgar Square au palais de St James au travers du quartier de la finance. Ce 11 juillet 2016, dans la luxueuse salle de conférences de James Hambro & Partners, la société de gestion de fortunes fondée par l'héritier de la banque Hambros, se presse tout un aréopage de financiers et d'avocats triés sur le volet et tirés à quatre épingles. On sert des cafés en attendant les présentations. La réunion est organisée par STEP, le syndicat des *family offices*, ces conseillers spécialisés dans l'administration de patrimoine des super-riches. L'objet du raout ? « Leçons panaméennes ». Sur la brochure de présentation, on peut lire : « La récente diffusion des Panama Papers a montré combien les données financières sont menacées par le cybercrime. Ce séminaire expliquera comment et pourquoi les cybercriminels ciblent les conseillers patrimoniaux. »

Les deux conférenciers tranchent sur l'assistance : cheveux courts et solidement bâtis, Jake Hockley et James Tamblin n'ont visiblement pas fait leur carrière dans la banque. Issus des services de renseignement britanniques, tous deux ont activement participé aux opérations clandestines du gouvernement de Sa Majesté, notamment en Irak et en Afghanistan. Et s'ils s'adressent aujourd'hui à la petite communauté des conseillers fiscaux et patrimoniaux de la place londonienne, c'est qu'après leur carrière militaire ils se sont reconvertis dans l'assistance aux grandes fortunes, qu'ils aident à protéger leurs données, leurs ordinateurs et leurs téléphones portables. Leur associé Oliver Crofton, visage rond chaussé de petites lunettes rondes, vient, lui, d'un autre monde : c'est un ancien hacker reconverti dans la protection numérique rapprochée. Sa spécialité : sécuriser les téléphones des actrices ciblées par les hackers en quête de photos intimes, et les ordinateurs des banquiers-stars terrifiés à l'idée que la presse apprenne les montants astronomiques de leurs bonus. Sous ses dehors inoffensifs, Oliver Crofton fut l'un des acteurs invisibles d'un des plus gros procès médiatiques de l'histoire britannique : celui qui opposa le tabloïd *News of the World* de Rupert Murdoch à un groupe de célébrités (Hugh Grant, Sienna Miller, Elle McPherson, etc.) dont les téléphones avaient été illégalement surveillés par des paparazzis. Crofton a aidé plusieurs des plaignants à prouver que les journalistes de *News of the World*, fermé

depuis, avaient illégalement accédé à leur messagerie et surveillé leurs appels.

Dans la salle de conférences de Pall Mall, Hockley, Tamblin et Crofton expliquent longuement aux gestionnaires des plus grosses fortunes de Londres comment protéger leurs serveurs et les BlackBerry de leurs clients. Les trois hommes illustrent leurs recommandations d'exemples précis, tous tirés d'affaires sur lesquelles ils sont intervenus. Mais ils évitent soigneusement d'évoquer le dernier dossier qui les occupe : comme vient de le révéler un entrefilet paru dans le *Sun*, les trois hommes travaillent en toute discrétion pour le sportif le plus célèbre (et le plus riche) de la planète, le footballeur David Beckham.

L'ancien attaquant de Manchester United est en effet, comme ses homologues Cristiano Ronaldo et Paul Pogba, menacé par une fuite massive qui s'apprête à dévoiler les coulisses les plus secrètes du foot-business. L'affaire obsède tout le microcosme de ce secteur, aussi épris de publicité dans les stades que discret sur ses finances. Rien n'est encore public, mais depuis le printemps plusieurs grands journaux européens (*Der Spiegel, El Mundo* et *L'Espresso*) épluchent huit disques durs contenant 18,6 millions de messages et de documents internes au fonds Doyen Sport, basé sur l'île de Malte et spécialisé dans les investissements dans les clubs de football. Les informations contenues dans ces disques sont suffisamment sensibles pour éclabousser tout l'univers du ballon rond, notamment Beckham. Le *Spice boy* a donc mandaté les trois limiers londoniens pour comprendre d'où vient la fuite et tenter d'en retarder la divulgation.

Inconnu du grand public, Doyen Sport est un rouage essentiel du financement sportif : le fonds a fait fortune en revendant des « parts de joueurs », une pratique controversée importée de la finance et finalement interdite en 2015. Cette activité consiste à avancer de l'argent à des clubs en difficulté en échange d'un pourcentage sur les contrats des footballeurs. Quand un joueur quitte une équipe pour une autre, une part du transfert revient à Doyen, qui récupère sa mise et souvent beaucoup plus. Mais Doyen joue également les banques d'affaires pour les clubs, qu'il aide à négocier des droits marketing, et conseille les joueurs sur leur patrimoine et leur droit à l'image. Simon Oliveira, le directeur opérationnel de Global, gère ainsi une partie des intérêts de David Beckham.

Centre névralgique du foot-business, Doyen Sport a subi une fuite massive de données à l'automne 2015. L'entreprise affirme qu'elle a été piratée et contacte plusieurs polices européennes. Si c'est effectivement un hack qui a visé Doyen, l'opération a été minutieusement préparée : en plus des e-mails et des documents stockés sur les serveurs de la société, les hackers ont également copié tous les messages échangés par l'équipe de Doyen Sport sur la messagerie cryptée WhatsApp. Ce qui représente un petit exploit, car, pour avoir accès à des messages WhatsApp, il faut soit disposer d'un accès au téléphone qui les envoie, pour les intercepter avant qu'ils ne soient cryptés, soit pirater les systèmes d'archivage en ligne, ou *cloud*, sur lesquels ils sont stockés. Bref, si c'est une équipe de hackers qui a attaqué Doyen Sport, ils n'en sont pas à leur coup d'essai.

Les assaillants disposent également d'une connaissance très fine de leur cible. Quelque temps après avoir attaqué Doyen, ils font fuiter plusieurs documents hackés sur un site portugais créé pour l'occasion, FootballLeaks. Une fois le message passé, ils s'adressent directement au fonds *via* l'hébergeur russe Yandex. Le message de leur porte-parole, qui se fait appeler Artem Lobuzov, est sans ambiguïté : « Tout cela, et bien plus, pourrait apparaître en ligne, puis dans la presse européenne. Vous n'en avez sûrement pas envie, pas vrai ? Mais on peut parler… » Pourquoi les maîtres chanteurs sont-ils si sûrs que Doyen va réagir ? Parce qu'ils savent que derrière l'usine à cash Doyen se cache un clan kazakh, les Arif, qui fuient maladivement la lumière. Or la peur de la publicité est ce qui attire les professionnels de la fuite massive. Certains des messages internes à Doyen montrent que la simple mention du nom des Arif dans une dépêche Bloomberg en juin 2013 a fait souffler un vent de panique au sein de Doyen. Qui sont les Arif ? Refik, le chef de clan, et ses trois frères, Rustem, Vakif et Tevfik, contrôlent l'usine kazakhe ACCP, spécialisée dans le traitement du chrome, dont le sous-sol du Kazakhstan regorge. Ils ont fait fructifier les revenus de ce complexe chimique en investissant dans l'immobilier, le négoce de matières premières, et surtout le sport, *via* Doyen. Mais les Arif ont toujours pris soin de faire profil bas : au Kazakhstan, on ne fait fortune que si l'on est protégé par le pouvoir et si l'on redistribue une partie des bénéfices à son protecteur. Ceux qui ont contrevenu à ces règles, tels Mukhtar Ablyazov et Viktor Krapunov, en ont été pour leurs frais. Pour ne pas exciter les convoitises, les Arif prennent

soin d’opérer derrière plusieurs écrans de sociétés offshore et s’astreignent à rester discrets : une fuite massive de leurs messageries signerait leur arrêt de mort.

Aussi, quand on leur propose de régler l’affaire contre paiement, ils acceptent sans barguigner. Artem Lobuzov, leur mystérieux interlocuteur, leur propose de détruire les informations piratées qu’il détient contre un versement compris entre 500 000 et un million d’euros. Une rencontre a lieu le 21 octobre dans une station-service à l’ouest de Lisbonne. Là, les émissaires de Doyen trouvent un avocat portugais qui se présente comme l’intermédiaire de Lobuzov, qualifié de hacker. Il leur fait une double proposition : soit Doyen paye 300 000 euros et les mails piratés seront détruits, soit le fonds recrute Lobuzov, qui deviendra leur hacker attitré.

Mais, déjouant les plans de leurs cyber-assaillants, les responsables de Doyen se sont rendus au rendez-vous équipés de micros cachés. La police écoute leur conversation avec les maîtres chanteurs, et la tentative d’extorsion tourne court. Trois mois plus tard, *Der Spiegel*, *El Mundo*, *L’Espresso* ou encore Mediapart reçoivent la totalité des messages piratés et commencent à les exploiter. En décembre 2016, ils publieront de manière coordonnée une rafale d’articles exposant tous les secrets de Doyen, les commissions payées en marge des transferts de joueurs et la fraude fiscale pratiquée à échelle industrielle. Les articles, accablants, susciteront l’ouverture d’enquêtes judiciaires en France et en Espagne, et signeront la mort de Doyen.

Il aura donc fallu moins d’un an, et un transfert de 1,9 gigaoctet de données, pour que le joyau de l’empire Arif explose. Qui a mené cette cyberfrappe chirurgicale et surtout pourquoi ? La police espagnole, saisie de plusieurs plaintes, mène l’enquête, tandis que les cyber-limiers londoniens recrutés par les joueurs éclaboussés par l’affaire, dont David Beckham, tentent eux aussi de remonter la piste. Jusqu’où mène-t-elle ? Les Arif sont des alliés fidèles de la présidence kazakhe : est-ce elle qui, à travers Doyen, est visée ? La chute de Doyen a en tout cas mis violemment en lumière les réseaux financiers du pouvoir kazakh, au moment où le pays tente de se refaire une virginité en sonnant à la porte de l’Organisation de coopération et de développement économique, le club des pays riches qui organise le G20.

L’épisode FootballLeaks montre en tout cas que la politique fait parfois un retour inopiné dans les opérations de diffusion massive de données commerciales. Forts de l’expérience acquise, ceux qui coordonnent les opérations de déstabilisation menées par les multinationales dans le cyberespace s’essaient parfois à monter des fuites massives contre des pays ou des groupes politiques. Avec des résultats mitigés. Illustration avec le très mystérieux Rinat Akhmetshin, le maître du « black P.R. », autrement dit de la destruction de réputation.

*

Le 9 juin 2016, deux visiteurs s’engouffrent dans l’ascenseur de la tour Trump à New York, symbole de l’empire du magnat de l’immobilier Donald Trump, qui vient deux semaines plus tôt d’être désigné comme candidat du Parti républicain à la présidentielle. Le premier, Natalia Veselnitskaya, est une avocate russe spécialisée dans les arbitrages internationaux et très proche du Kremlin. L’autre, Rinat Akhmetshin, est un ancien soldat de l’Armée rouge reconverti dans la communication de crise et naturalisé américain. Les deux invités montent jusqu’au 25e étage, où ils ont rendez-vous avec Donald Trump junior, le fils aîné du candidat, ainsi que son gendre, Jared Kushner. Selon des e-mails révélés par le *New York Times*, les deux consultants sont venus proposer à l’équipe Trump des « informations compromettantes sur la campagne de Hillary Clinton ». Un mois plus tard, WikiLeaks publie le contenu des messageries privées des conseillers de la candidate démocrate et fait basculer la course à la Maison-Blanche.

L’objet des conversations, ce jour-là, entre l’entourage de Trump et les deux consultants fait l’objet de multiples investigations du Congrès, mais également du renseignement américain, qui cherche à déterminer si le piratage des e-mails du Parti démocrate a été téléguidé par la Russie avec la complicité tacite du candidat républicain. Une chose est sûre : Rinat Akhmetshin, l’un des deux invités à la tour Trump ce jour-là, est une sommité dans le petit monde de la fuite massive. Il a été mêlé à plusieurs affaires de divulgation de messagerie pour le compte d’entreprises privées.

La plus emblématique est l'opération montée en 2013 pour le compte d'EuroChem-VolgaKaliy, un conglomérat minier contrôlé par un oligarque russe proche du Kremlin, Andrey Melnichenko. En 2012, EuroChem porte plainte contre un de ses partenaires, la société International Mineral Resources (IMR), lui réclamant un milliard de dollars de dommages et intérêts. Celle-ci compte parmi ses actionnaires l'homme d'affaires kazakh Patov Chodiev, lui-même victime de plusieurs tentatives de piratage.

Mais le procès se passe plus mal que prévu, et EuroChem peine à faire valoir ses droits. Ce premier échec oblige les belligérants à changer de tactique : dès l'année suivante, IMR voit des documents internes à l'entreprise apparaître dans la presse internationale, notamment dans le magazine américain *Harper's*. Persuadée qu'elle a été piratée, la société minière diligente des investigations internes, confiées à un petit cabinet d'enquête privé américain, GlobalSource. Comme nous avons pu le constater à de nombreuses reprises au cours de notre enquête, ces consultants discrets ont une connaissance particulièrement fine du marché mondial de la piraterie informatique. Grâce à ses réseaux, GlobalSource parvient à racheter une copie des dossiers subtilisés sur les réseaux d'IMR. À l'examen, ces pièces révèlent des traces de manipulation par un individu dont les initiales sont R. A. Pourrait-il s'agir de Rinat Akhmetshin ? Le consultant dispose d'un contrat de consultant avec les avocats de Salisbury & Ryan, qui conseillent EuroChem. Pour en avoir le cœur net, les enquêteurs de GlobalSource ont recours à une technique désuète, mais éprouvée : ils mettent Rinat Akhmetshin sous surveillance et le suivent dans ses déplacements, notamment à Londres. Là, caché dans la pénombre d'un café, ils l'observeront transmettre à plusieurs interlocuteurs une clé USB contenant 50 gigaoctets de données piratées chez IMR.

La société ciblée porte plainte à Washington, obligeant Rinat Akhmetshin à reconnaître qu'il est bien en possession de données hackées sur ses serveurs. Il niera cependant avoir commandité le moindre piratage, affirmant avoir acheté les documents sur le « marché parallèle de l'information ». Dans une conversation surprise par les enquêteurs de GlobalSource au Café Royal sur Regent Street, à Londres, Rinat Akhmetshin affirmait pourtant à un interlocuteur avoir « payé beaucoup d'argent » à des hackers russes pour qu'ils piratent les messageries d'IMR…

C’est le même personnage qui réapparaîtra deux ans plus tard dans une réunion au sommet entre une avocate russe et les conseillers de Donald Trump, réunion consacrée au partage d’informations « gênantes » pour Hillary Clinton. S’agit-il, là encore, de préparatifs d’une fuite massive, celle que relayera un mois et demi plus tard WikiLeaks ? C’est ce que les enquêteurs du Congrès américain tentent de savoir.

Inventée par d’authentiques lanceurs d’alerte, la technique de la fuite massive s’est ainsi rapidement dévoyée. On recense aujourd’hui plus de fuites liées à des conflits financiers entre entreprises et grandes fortunes que de révélations motivées par des objectifs politiques. La fuite massive de données est entrée dans l’arsenal de la guerre économique et patrimoniale, comme elle a été récupérée par les États pour pousser leurs intérêts. Petit à petit, les porte-flingues remplacent les lanceurs d’alerte, obligeant les journalistes qui exploitent les données volées à se poser de plus en plus de questions sur les motivations de ceux qui leur apportent, clé en main, des gigaoctets de messages confidentiels.

Questions d’autant plus tentantes à évacuer que, souvent, elles sont insolubles et peuvent sembler accessoires. La principale qualité d’une fuite, on l’a souvent répété au cours de cette enquête, c’est de ne porter que sur des documents authentiques. Si les pièces sont vraies, et d’intérêt public, pourquoi s’inquiéter de l’identité de ceux qui les manipulent ? Les « leaks » ont une autre qualité pour les journalistes : ce sont des histoires complètes, qui demandent peu de vérifications ultérieures. Il suffit de les lire et de les recouper pour avoir une mine inépuisable de scoops. Dans ces conditions, à quoi bon s’interroger sur leur provenance, au risque de voir la manne s’échapper et être proposée à d’autres médias ? Car les opérateurs de fuites connaissent bien la presse, structurellement concurrentielle. Avant de proposer ses données à la *SonntagsZeitung*, le « John Doe » des Panama Papers avait ainsi contacté le *New York Times* et le *Washington Post*, qui se sont ensuite mordu les doigts d’avoir laissé échapper un pareil trésor.

VI

Les blanchisseurs

Une fuite massive est avant tout une opération clandestine : les pirates qui volent les données, comme les stratèges qui les mandatent, opèrent dans l'ombre et s'ingénient à brouiller les pistes pour masquer leur intervention. Mais, pour atteindre leur objectif et déstabiliser leur cible, ces cybercommandos ont besoin d'un relais qui, lui, soit public : un site Internet, ou mieux un journal à la réputation bien établie, qui publiera les documents piratés, authentifiera leur contenu et développera, à l'attention du public non averti, les informations gênantes qu'ils contiennent. Bref, si la fuite massive est une arme, elle n'est rien sans détonateur médiatique.

C'est le porte-voix qui transforme les données brutes en scandale et légitime la violation du secret au nom de la valeur des informations révélées et de l'intérêt qu'elles présentent pour le public. Pour le commanditaire d'une fuite, un bon relais est un relais qui dispose d'une audience mondiale et d'une réputation sans tache, mais sait se montrer suffisamment pugnace pour accepter de publier des informations confidentielles dont il ignore la provenance.

De 2006 à 2011, le premier de ces relais a été le site WikiLeaks, qui a littéralement inventé la fonction d'éditeur de fuite massive et la marque -leaks, déclinée *ad nauseam* depuis. À mesure que l'organisation de Julian Assange perdait de son lustre, elle a été remplacée par d'autres plateformes, moins militantes et plus collaboratives.

Mais la véritable chambre de détonation d'une fuite massive, ce sont les médias dans leur ensemble. Ce sont eux qui vont relayer et amplifier l'impact des informations volées en multipliant les manchettes et les articles. Un journaliste, nous sommes bien placés pour l'écrire, est tout autant incapable de résister à une masse d'informations confidentielles et

véridiques qu'un enfant à un pot de Nutella géant. Et ceux qui prétendent le contraire sont des menteurs, trahis par leur moustache en chocolat.

*

Ce sont le visage public des fuites : WikiLeaks, Cryptome, International Consortium of Investigative Journalist, European Investigative Consortium, DCLeaks… Ils sont la cheville ouvrière et, bien souvent, la seule manifestation identifiée du phénomène des fuites massives. Toutes ces plateformes Internet ont été mises en place pour publier et indexer des documents secrets, confidentiels ou simplement privés.

Les rares ouvrages traitant des fuites massives, publiés aux États-Unis ou au Royaume-Uni, sont tout entiers consacrés à ces sites. Or, comme nous avons tenté de le mettre en évidence dans les chapitres précédents, ils sont un maillon, certes essentiel, mais en aucun cas déterminant dans la longue chaîne de distribution des données protégées.

Ces sites, et les organisations qui les animent, fonctionnent tous de manière identique. Pour être efficaces, c'est-à-dire divulguer d'un coup et à l'échelle mondiale une masse considérable d'informations secrètes, ils doivent être :

1 – Visibles et bien référencés sur les moteurs de recherche comme Google ;

2 – Fournir un système de recherche et d'indexation efficace, pour que les utilisateurs aient la possibilité de naviguer dans la base de données publiée ;

3 – Et, surtout, placer un mur inviolable entre l'origine de l'information et les lecteurs, ce afin que jamais la source des documents publiés ne puisse être identifiée. Au risque d'alimenter les hypothèses les plus folles sur la provenance des données.

Mal équipés pour une telle mission, les médias traditionnels se sont vite retrouvés débordés sur le créneau des fuites massives par de nouveaux acteurs digitaux et militants. Volontiers méfiants, voire ouvertement

critiques envers les journalistes, cette génération d'*hacktivistes*, comme ils aiment à se baptiser eux-mêmes, a développé tout un discours pour justifier ses pratiques, insistant notamment sur l'utilité citoyenne des fuites, la nature profondément antidémocratique du secret et la nécessité de la transparence, vecteur ultime de changement. Quand on l'interroge sur son plus grand succès, Julian Assange, le fondateur de WikiLeaks, cite toujours le « printemps arabe », intervenu après la publication de 251 287 télégrammes diplomatiques américains sur son site : en Tunisie et en Égypte, la révélation de la collusion des régimes en place avec Washington a effectivement accéléré leur chute.

Mais ce discours a un corollaire : pour justifier les fuites, et donc leur existence, ces plateformes Internet répugnent souvent à enquêter sur l'origine des données qui leur sont fournies, et plus encore sur les éventuelles motivations de leurs informateurs, préférant se concentrer sur l'examen minutieux des dossiers reçus. Il faut le redire, et très clairement : ce n'est pas parce qu'un informateur a un dessein caché que les pièces qu'il transmet sont manipulées. Toutes les fuites recensées dans cet ouvrage ne portent que sur des éléments authentiques, et dignes d'intérêt. Malgré les dénégations du département d'État, les télégrammes diplomatiques américains publiés par WikiLeaks étaient véridiques et riches en révélations, tout comme les 11,5 millions d'actes du cabinet panaméen Mossack Fonseca mis en ligne par l'International Consortium of Investigative Journalists (ICIJ). Pourtant, malgré leur valeur intrinsèque, ces documents ne constituent bien souvent qu'une partie de l'événement : les e-mails internes du Parti démocrate publiés par WikiLeaks à la veille de l'élection présidentielle américaine étaient moins intéressants en eux-mêmes que les objectifs de ceux qui les ont piratés. Plus d'un an après leur divulgation, on parle toujours, à Washington, de l'interférence russe dans la campagne américaine, et plus du tout du contenu des échanges du staff de campagne de Hillary Clinton.

Il ne s'agit pas ici de faire le procès de cette nouvelle génération de chasseurs de secrets : leurs tropismes sont aussi, bien souvent, les nôtres. Il s'agit simplement de montrer que, au-delà de leurs vœux de transparence, ces professionnels de la révélation digitale ont aussi une histoire et qu'ils participent d'un phénomène plus large dans lequel ils sont certes des aiguilleurs, mais jamais les décideurs.

* * *

La scène a lieu à Ellingham Hall, un manoir de famille situé dans le Norfolk, au Royaume-Uni. La propriété appartient à la famille de Vaughan Smith, un ancien grenadier de la reine devenu correspondant de guerre. Fondateur du très select Frontline Club, une association de journalistes calquée sur le modèle des clubs londoniens, Smith est issu de la plus haute aristocratie britannique : son père était le messager personnel de la reine. Au début de l'année 2011, Smith héberge le fondateur de WikiLeaks, l'Australien Julian Assange, sous le coup d'une assignation à domicile pour agression sexuelle en Suède (vivement contestée par l'intéressé, la procédure sera abandonnée six ans plus tard, une partie des faits étant prescrits).

Ce 23 juin 2011, Ellingham Hall reçoit un hôte de marque : Eric Schmidt, le PDG de Google. Figurant parmi les dirigeants les plus célèbres et les plus riches de la planète, Schmidt est venu interviewer Assange pour un livre de prospective (*Le Nouvel Âge digital*, publié en 2013). L'apôtre australien du « Leak », plus porté sur les discours que sur la discussion (sollicité à plusieurs reprises pour ce livre, il n'a pas donné suite à nos demandes de rencontre), a fait une exception pour Google. Les trois heures de conversation qui vont suivre, parfois surréalistes, constituent un témoignage précieux sur l'esprit du projet WikiLeaks : « Tout autour du monde, il y a des gens qui observent différents aspects de leur réalité locale. Et il y a d'autres gens qui reçoivent des informations dont ils n'ont pas fait l'expérience eux-mêmes. Et au milieu, il y a des gens qui passent des informations depuis les observateurs jusqu'aux gens qui vont agir sur la base de ces informations (…). Des entreprises comme Google, par exemple, sont engagées dans cette intermédiation entre les gens qui ont l'information et ceux qui la veulent. » Eh bien, c'est pareil pour WikiLeaks, explique en substance Assange à Eric Schmidt : le site de diffusion de fuites massives est un « système total ».

Il y a quelque chose d'un peu déconcertant à écouter une figure plus généralement identifiée avec la subversion tous azimuts décrire son projet en termes monopolistiques et le comparer à celui de l'entreprise la plus intégrée dans l'économie mondiale. Mais l'équation est révélatrice à bien

des égards : comme Google, WikiLeaks est une place d'échange qui vise à supprimer les intermédiaires – en l'occurrence, les journalistes – et à mettre en place un monopole, celui du courtage de l'information brute. Et Assange, comme Schmidt, est un entrepreneur : d'un projet, d'abord, mais aussi et surtout de lui-même.

Autodidacte, Assange s'est passionné dès les années 1980 pour l'informatique et le piratage sous le pseudonyme de Mendax. Mais, à rebours des pionniers du hacking, plutôt portés sur l'anonymat, il s'est très tôt soucié de sa légende : au milieu des années 1990, il est le héros d'un livre, *Underground*, qu'il coécrit lui-même avec la journaliste australienne Suelette Dreyfus. Cet ouvrage fait de lui le héros de la cyberfrontière. Il raconte comment, âgé de 16 ans, il s'est introduit dans les réseaux du géant des télécommunications américain, Nortel, mais aussi de la NASA et du Pentagone, et a finalement été arrêté pour avoir pénétré le système de l'opérateur téléphonique australien Minerva. Condamné à une amende, Assange se passionne ensuite pour la science du secret, la cryptographie, et contribue régulièrement au célèbre forum de discussion Cypherpunks, alors fréquenté par tous les activistes de la protection de la vie privée.

Comme Bill Gates ou Eric Schmidt, Assange n'est pas l'inventeur du concept qui l'a rendu célèbre. L'idée d'une plateforme Internet spécialisée dans la publication brute de documents secrets est celle d'un architecte américain, John Young, également abonné au forum Cypherpunks. En 1996, Young met en place un site, cryptome.org, qui publie d'abord des manuels et des recherches confidentielles sur la cryptographie, puis, très vite, toutes sortes d'informations protégées : des listes de noms d'agents du MI6, l'agence du renseignement extérieur britannique, ainsi que d'informateurs de la CIA et de leurs adresses personnelles. Young, comme plus tard Assange, ne croit qu'à l'information brute et refuse obstinément toute censure et toute mise en perspective de l'information. Dix ans après avoir lancé Cryptome, il est contacté par Julian Assange qui lui propose d'être l'administrateur d'un « projet de fuite de masse » baptisé WikiLeaks et dont les serveurs seront masqués derrière un paravent électronique.

Plus que l'idée, c'est le fonctionnement du site qui est révolutionnaire – Eric Schmidt et Julian Assange, tous deux techniciens de l'informatique, consacrent d'ailleurs plus de la moitié de leurs échanges à ces questions

d’architecture réseau. L’anonymat des sources, des visiteurs et des administrateurs est méticuleusement protégé. Chaque consultation du site génère un échange aléatoire de données entre les serveurs de WikiLeaks et l’ordinateur de l’internaute, ce qui, pour un observateur extérieur, fait de chaque visiteur un informateur potentiel et noie ceux qui envoient effectivement des documents à WikiLeaks dans un océan de données. Le site lui-même utilise un outil, Tor, qui rend la localisation de ses serveurs virtuellement impossible. Mis en place dans les années 1990 sur financement de la DARPA, le laboratoire du Pentagone, Tor est un système de transmission de données qui utilise Internet, mais fonctionne en parallèle au réseau des réseaux. Constitué de milliers de volontaires, c’est un ensemble de relais électroniques qui, chacun, réceptionnent et renvoient des informations de manière aléatoire en cryptant à chaque fois leur origine et leur destination. Tous les échanges qui empruntent Tor, qu’il s’agisse de requêtes vers un site Internet, de messages ou de transferts de fichiers, voient l’identité de leur émetteur et de leur destinataire codée et surcodée, ce qui rend toute identification absolument impossible.

À la fin de l’année 2006, wikileaks.org fait son apparition sur Internet.

* * *

Disposant de l’outil dont il rêvait, Julian Assange doit désormais l’alimenter : une plateforme de fuite massive qui ne publie pas de secrets n’est rien d’autre qu’une boîte de nuit vide. Pendant deux ans, Julian Assange va donc se transformer en homme-sandwich et parcourir le monde, enchaînant les conférences et les *workshops* pour imposer son idée. Son discours, à l’époque, ressemble peu ou prou à la campagne marketing d’une start-up : il affirme recevoir « des milliers de documents par jour » et travailler avec des « centaines de volontaires » à travers le monde. Pourtant, partout où WikiLeaks est invité, Assange se présente toujours seul, et son site ne publie qu’une poignée de documents anecdotiques : un projet d’assassinat de leader somalien qui a toutes les apparences d’un faux, des documents sur les fraternités d’étudiants américains, des manuels administratifs et des listes de sites censurés par des fournisseurs d’Internet… Bref, rien qui ne distingue WikiLeaks des milliers de sites simili-conspirationnistes qui prolifèrent partout sur la Toile.

À force de persévérance, WikiLeaks réussit cependant à frapper deux grands coups successifs en 2007 et 2008. Étonnamment, aucune de ces fuites ne passe par les systèmes d'anonymisation sophistiqués développés par Assange. En 2007, ce sont des activistes kenyans qui lui remettent, de la main à la main, un long rapport confidentiel commandité par leur gouvernement au cabinet d'enquête privé Kroll et consacré aux détournements opérés par l'administration du président Daniel Arap Moi, qui vient de quitter le pouvoir. L'année suivante, le responsable de la banque Julius Baer aux îles Caïmans, Rudolf Elmer, fournit très publiquement au site des centaines de documents sur les trusts anonymes mis en place par l'établissement suisse pour ses clients les plus riches. Les deux publications sont largement reprises par la presse et WikiLeaks parvient, enfin, à imposer sa marque. Suivront des manuels internes à l'Église de scientologie et des milliers de copies de messages instantanés envoyés et reçus par les équipes de secours dépêchées sur le World Trade Center le 11 septembre 2011.

Au début de l'année 2010, WikiLeaks n'est plus seulement un site : c'est désormais une marque, un projet, et surtout un visage, celui, pâle et encadré de longs cheveux blancs, de Julian Assange. La légende du Steve Jobs de la fuite massive a remplacé celle du prodige du hacking. La réalité, elle, reste toujours aussi fluctuante.

Moins d'un an plus tard, en décembre 2010, Assange fera la couverture du magazine américain *Time*, comme Steve Jobs en son temps. Entre-temps, WikiLeaks aura publié, en quatre salves successives, une vidéo montrant un hélicoptère militaire américain tirant sur des employés de l'agence de presse Reuters en Irak ; des centaines de milliers de rapports d'activité d'unités militaires américaines actives en Afghanistan et en Irak ; et, en novembre 2010, 251 287 télégrammes confidentiels rédigés par la diplomatie américaine durant près de trente ans. En huit mois, le site est devenu un phénomène mondial, et Julian Assange, une star. Un succès imputable non à des « centaines de sources », comme ne cesse de le répéter Assange, mais à un seul homme, Bradley Manning, un jeune militaire américain en poste en Irak. Analyste dans les renseignements militaires, Manning a copié, puis transmis à WikiLeaks l'intégralité des documents confidentiels publiés par le site en 2010. Manning est arrêté en juin 2010

après s’être confié à un hacker qui le dénoncera au FBI. Ayant changé de genre en prison, Bradley, devenu Chelsea, a finalement été gracié par Barack Obama à la fin de son mandat et libéré de prison en mai 2017.

Cette série de méga-scoops établit la réputation de Julian Assange tout aussi rapidement qu’elle précipite sa chute. Au vu de la masse d’informations reçues, WikiLeaks, dont « l’équipe mondiale » reste toujours aussi squelettique et composée, pour l’essentiel, d’informaticiens peu au fait des subtilités de la géopolitique, n’a en effet d’autre solution que d’oublier ses préventions contre les médias et de s’associer avec plusieurs d’entre eux pour éplucher les documents fournis par Manning. Le *Guardian* est le premier à proposer en juin 2010 à WikiLeaks un partenariat pour exploiter la base de données des rapports militaires américains en Irak et en Afghanistan. L’offre du quotidien est simple : ses journalistes analyseront les documents et rédigeront des articles et, le jour de leur publication, WikiLeaks mettra en ligne les pièces originales.

Mais rien ne se passe comme prévu. L’association, vite élargie au *Spiegel* allemand et au *New York Times*, est envisagée par les trois quotidiens comme une collaboration. Mais Assange, lui, la considère plutôt comme un contrat de sous-traitance. Comme le racontent les journalistes du *Guardian* David Leigh et Luke Harding dans leur livre *WikiLeaks: Inside Julian Assange’s War on Secracy* (2013), entièrement consacré à cette période, le fondateur de WikiLeaks n’aura de cesse de leur dicter des conditions de travail et de publication, qu’il exige de voir appliquées à la lettre, faute de quoi il menace de reprendre le contrôle des documents fournis. Fidèle à ses principes de transparence absolue, Assange commence notamment par s’opposer à la censure de certains documents, tandis que les journalistes, eux, veulent masquer des noms des informateurs irakiens et afghans qui sont en lien avec l’armée américaine, par peur d’exposer ces individus à des représailles. Les quotidiens auront finalement gain de cause, mais Assange se pliera à leur exigence de très mauvaise grâce.

Quand il peine à imposer ses vues, Assange joue les médias les uns contre les autres, passant des partenariats avec de nouveaux titres sans informer les autres. En juillet 2010, à la veille de la publication des documents militaires américains sur l’Afghanistan dans le *Guardian*, il transmet ainsi une partie de la base de données, dûment classée et éditée par

les journalistes du quotidien, à la chaîne de télévision Channel 4… En octobre 2010, l'exploitation des rapports sur l'Irak sera encore plus chaotique : Assange veut contraindre les trois journaux à reculer la date de publication de six semaines pour permettre à une société de production qu'il a choisie de faire un documentaire. Puis il se rapproche d'Al-Jazeera, qui annoncera la fuite des documents irakiens une heure avant le *Guardian* et le *New York Times*, pourtant partenaires de WikiLeaks…

À l'automne 2010, lorsque les trois quotidiens commencent à s'atteler aux télégrammes diplomatiques transmis par Manning à WikiLeaks, leur partenariat avec Julian Assange s'est transformé en mariage dysfonctionnel. L'*hacktiviste* australien, mécontent d'un portrait qui lui a été consacré dans le *New York Times*, exige que le journal soit exclu de la collaboration et remplacé par le *Washington Post*. Mais la désorganisation suscitée par WikiLeaks se retourne contre lui. Par le biais d'un volontaire de l'organisation, le *Guardian* a en effet obtenu une autre copie de la base de données des télégrammes et résiste au chantage d'Assange. Celui-ci fait marche arrière, mais impose néanmoins que l'association soit élargie à deux autres journaux : *Le Monde* et *El País*.

La publication des télégrammes diplomatiques le 28 novembre 2010 se solde par une déflagration planétaire, vigoureusement dénoncée par l'administration Obama. Mais elle aura un effet retour tout aussi violent sur WikiLeaks. Plusieurs militants historiques, parmi lesquels l'Allemand Daniel Domscheit-Berg, quittent l'organisation, dénonçant le leadership « dictatorial » de Julian Assange. Ils emportent avec eux toute la base de données de l'organisation et, surtout, le logiciel qui permet aux contributeurs du site d'envoyer des documents en toute sécurité. Autrement dit, le cœur du réacteur de l'organisation… Ce système de soumission anonyme, fierté d'Assange, reste fermé pendant quatre ans, jusqu'en mai 2015. Quant à la base de données, elle est récupérée par WikiLeaks au terme d'une longue négociation arbitrée par le Chaos Computer Club, le légendaire groupe de hackers de Berlin, et remise en ligne en 2011 sur le site de téléchargement illégal The Pirate Bay. Problème : les documents publiés sont les originaux, et non les copies patiemment censurées par les journalistes du *Guardian* pour protéger l'identité des informateurs de l'armée américaine… En quelques jours, des centaines d'individus verront

leurs liens avec les États-Unis exposés sur Internet et devront tout abandonner pour rester en vie. Suite à ces épisodes, aucun des grands médias européens ayant travaillé avec WikiLeaks n'acceptera de renouveler l'expérience.

Renvoyé à son splendide isolement, Julian Assange se retrouve également visé par deux procédures judiciaires. La première est une enquête préliminaire initiée par les États-Unis, qui étudient la possibilité d'accuser Assange d'espionnage pour avoir activement aidé Manning à dupliquer des documents secrets lorsque ce dernier était en poste en Irak. Lors du procès de Manning devant la justice militaire, des copies de messages instantanés retrouvés sur l'ordinateur du soldat montrent en effet qu'il a correspondu avec un militant de WikiLeaks – mais s'agit-il d'Assange ? – et que ce dernier l'a aidé à deviner un mot de passe sur le réseau militaire, opération qui a permis au soldat d'accéder aux documents confidentiels publiés plus tard par le site.

L'autre procédure est plus gênante pour Assange : elle émane de Suède, où WikiLeaks a longtemps caché ses serveurs derrière de multiples couches de leurres électroniques. En 2010, un procureur suédois accuse le fondateur de WikiLeaks d'avoir eu des rapports sexuels non consentis et non protégés avec deux femmes. Assange dénonce une procédure manipulée par les autorités américaines et refuse de se rendre aux convocations de Stockholm, affirmant qu'il court le risque d'une extradition vers les États-Unis. Sur injonction judiciaire suédoise, il est assigné à résidence au Royaume-Uni. L'affaire écorne sa réputation, jusqu'ici immaculée. En 2017, la journaliste Laura Poitras enfoncera le clou dans un documentaire montrant que WikiLeaks baigne dans une culture éminemment machiste. La charge de Poitras sera particulièrement dommageable pour WikiLeaks : acquise à la cause de la fuite massive, Poitras a été choisie par Edward Snowden pour relayer ses premières révélations. Elle en tirera un film, *Citizen Four*, couronné d'un Oscar. Mais Poitras, qui a un temps vécu avec Jacob Appelbaum, le représentant de WikiLeaks aux États-Unis, a découvert, à mesure qu'elle a pénétré au sein de l'organisation, une atmosphère très différente de celle qu'elle avait imaginée. La violence des relations interpersonnelles à l'intérieur de WikiLeaks la fait déchanter comme, avant elle, les militants qui ont abandonné Assange en 2011.

L’enquête sur les agressions commises par Assange en Suède n’a pas pour seul effet de ternir son image. Elle prive également le fondateur de WikiLeaks de sa liberté de mouvement et le place dans une situation éminemment précaire. Pour se sortir d’affaire, il aura recours à quelques techniques éprouvées, et notamment l’instrumentalisation des médias, qui, tous, brûlent de relayer les documents accumulés par son organisation et dont Assange dispose comme d’une cassette personnelle. En France, *Le Monde* publiera ainsi une lettre ouverte du fondateur de WikiLeaks à François Hollande dans laquelle Assange demande au président français de lui accorder l’asile politique, « sa vie étant aujourd’hui en danger ».

Dernière conséquence, et non des moindres, de la publication en rafale des documents de Bradley Manning : les banques et les services de transfert d’argent en ligne comme PayPal refusent de relayer les dons à WikiLeaks. Au moment où elle est le plus active et le plus visible, l’organisation se voit interdire toute levée de fonds et court donc le risque d’un étranglement financier.

L’affaiblissement généralisé de WikiLeaks fait de l’organisation une cible idéale pour les gouvernements qui souhaitent s’approprier le formidable porte-voix mis en place par Julian Assange. C’est notamment le cas de la Russie, qui travaille depuis plusieurs années à intégrer le piratage informatique et la fuite massive à son arsenal de propagande clandestine. Dès 2010, l’administration Poutine se met donc en branle pour se rapprocher d’Assange, lui offrant, comme nous l’avons vu, des soutiens, un contrat de présentateur pour regarnir son compte en banque et, surtout, un refuge dans l’ambassade londonienne de son allié équatorien. Grâce à l’action de Moscou, le fondateur de WikiLeaks est mis à l’abri de toute demande d’extradition, qu’elle émane de la Suède ou des États-Unis.

Protégé par un gouvernement lié à Moscou et intervenant à la télévision d’État russe, Assange aligne alors l’activité de WikiLeaks sur les intérêts de son puissant parrain. À partir de 2011, toutes les fuites massives publiées par WikiLeaks, à l’exception d’une seule, ne ciblent que les États-Unis. Mieux, dès l’année suivante, WikiLeaks joue, on l’a vu, un rôle déterminant dans l’opération d’aiguillage d’Edward Snowden vers Moscou.

À partir de cette époque, WikiLeaks va également développer un tropisme très prononcé pour les coulisses des consultations électorales. En

2016, le site tente de torpiller la candidature présidentielle de Hillary Clinton, violemment antirusse, en publiant les messages internes de son parti sur son site. La même année, WikiLeaks offre 200 000 livres sterling à tout informateur à même de lui fournir des informations sur d'éventuelles manœuvres des dirigeants du Parti travailliste anglais pour écarter Jeremy Corbyn de la primaire. Arrivé en tête du vote des militants en septembre 2015, Corbyn, qui a les faveurs de la Russie, car il est viscéralement pacifiste et donc opposé à l'OTAN, a vu sa base électorale purgée par le leadership de son parti et risque de perdre la primaire. Malgré la prime offerte par le site, qui, quelques années auparavant, frisait la banqueroute, WikiLeaks ne recevra aucune information et Corbyn remporte *in extremis* la primaire, mais perd les élections en 2017. Enfin, en juillet 2017, l'organisation de Julian Assange publie l'intégralité des mails internes au parti En marche ! d'Emmanuel Macron, ouvertement critique vis-à-vis de Moscou.

Est-ce à dire, comme nous avons entendu le directeur de la CIA l'affirmer à Washington, que Julian Assange est un agent russe ? Aucun élément tangible ne permet de l'affirmer avec certitude, et l'accusation paraît de toute façon simpliste, voire caricaturale : Assange, on l'a vu au début de ce chapitre, est avant tout préoccupé de son image et du succès de son entreprise. Que ce narcissisme constitue une faiblesse que Moscou ait su utiliser à bon escient pour attirer Assange dans son orbite semble beaucoup plus vraisemblable. Tout comme le fait que le rapprochement avec la Russie ne soit, pour WikiLeaks, qu'une alliance tactique et non un mariage éternel. En septembre 2017, comprenant que sa proximité avec le Kremlin devient de plus en plus visible, Assange tente de ripoliner son image en publiant, sous le nom de « Spy Files Russia », une série de documents internes aux principales entreprises de surveillance électronique russes. Mais l'opération, relayée par deux journaux seulement, peine à faire des vagues : les dossiers publiés sont, on l'a vu, anecdotiques, et ne suscitent aucune réaction.

*

La disgrâce de WikiLeaks ouvre la voie à de nouveaux professionnels de la fuite, moins militants et plus intégrés à la communauté journalistique. Pour tous les médias qui ont collaboré à la publication des télégrammes diplomatiques américains et, plus tard, à celle des documents volés par Edward Snowden, le principal enseignement de ces aventures est qu'une fuite massive ne peut être efficacement traitée par une seule rédaction et doit nécessairement impliquer une coalition internationale de journalistes ainsi que des outils professionnels de gestion de base de données.

C'est le Center for Public Integrity (CPI), une organisation américaine fondée par l'ancien producteur de « 60 Minutes » Charles Lewis, qui va mettre en place la première coopérative destinée au traitement de fuites massives et prendre ainsi la place laissée vacante par WikiLeaks. Depuis le début des années 1990, le CPI enquête sur l'industrie du lobbying à Washington et publie une base de données très complète, compilée à partir de sources publiques. Elle recense tous les lobbyistes recrutés pour défendre les intérêts des grandes entreprises américaines au Congrès, et les dons qu'ils effectuent aux campagnes des hommes politiques. Grâce à cette expérience de traitement d'informations, mais également grâce aux dons des nombreuses fondations philanthropiques qui l'épaulent, le CPI a créé une branche internationale, l'International Consortium of Investigative Journalist (ICIJ), qui va se doter d'une plateforme collaborative ultra-sécurisée, de coûteux logiciels d'indexation de données, parmi lesquels le programme australien Nuix et le système américain dtSearch, et d'un répertoire mondial de journalistes d'enquête. Contrairement à WikiLeaks, l'ICIJ ne se destine pas à opérer seul, mais simplement à offrir une résidence virtuelle aux journalistes désireux d'exploiter efficacement les téraoctets de documents confidentiels qu'ils ont reçus. Autre différence avec l'organisation de Julian Assange, l'ICIJ refuse de publier des données brutes et s'astreint à ne mettre en ligne que des documents dont la véracité et surtout la pertinence ont été établies au préalable par des journalistes. En revanche, l'organisation retient de l'expérience WikiLeaks la nécessité de nouer des partenariats exclusifs avec un média par pays. Une politique qui suscite, dans plusieurs capitales, une vigoureuse bataille entre médias pour être le seul titre agréé par l'ICIJ. La franchise ICIJ garantit en effet à ceux qui l'obtiennent un accès privilégié aux documents traités par l'organisation et leur confère un avantage décisif dans le traitement d'affaires au retentissement mondial. Un sésame que *Le Monde*, en France, s'est battu

pour obtenir. En réaction à leur exclusion de l'ICIJ, plusieurs médias mettent en place des organisations concurrentes, notamment l'European Investigative Collaborations, initié par *Der Spiegel* et qui révélera les Football Leaks.

Et ce modèle fonctionne : entre 2013 et 2016, l'ICIJ, en association avec la *Süddestche Zeitung*, le *Guardian* et *Le Monde*, publie trois fuites massives sur les paradis fiscaux au retentissement planétaire : d'abord Offshore Leaks, qui compile 260 gigaoctets de documents et d'e-mails internes à deux cabinets d'enregistrement de sociétés offshore, Portcullis Trustnet, basé à Singapour, et Commonwealth Trust Limited, établi dans les îles Vierges britanniques. En 2014, l'ICIJ divulgue 28 000 pages d'accords fiscaux préférentiels négociés pour le compte de grandes entreprises – Apple, McDonald's, etc. – par l'antenne luxembourgeoise du cabinet d'audit PricewaterHouseCoopers (PWC). Les données ont été clandestinement fournies à l'ICIJ par deux salariés de PWC, Antoine Delcour et Raphaël Halet, qui n'ont reçu aucune rétribution, ont agi de leur propre initiative et, comme Bradley Manning, seront traduits en justice au Luxembourg et condamnés pour leurs actes. Enfin, en 2016, l'ICIJ publie 2,6 téraoctets de données, e-mails et documents issus du cabinet panaméen Mossack Fonseca, lui aussi spécialisé dans les sociétés offshore. Dans cette opération, l'ICIJ n'était pas destinataire des données : celles-ci ont été apportées par l'un des journaux membres de l'organisation, le quotidien allemand *SonntagsZeitung*, qui les a partagées avec les autres membres. L'ICIJ s'est contentée d'apporter un soutien logistique et de superviser la répartition du travail entre les journaux membres.

Contrairement aux documents publiés par WikiLeaks, les fuites massives divulguées par l'ICIJ n'épargnent pas la Russie. En 2013, les Offshore Leaks montrent ainsi que plusieurs intimes de Vladimir Poutine, notamment Valentin Golubev, le président du comité exécutif de la société d'État russe Gazprom, ont des sociétés offshore aux îles Vierges britanniques. En 2016, les Panama Papers enfoncent le clou : les documents de Mossack Fonseca révèlent que Serguei Roldugin, un violoncelliste intime de Poutine, dispose de sociétés panaméennes qui gèrent près de deux milliards de dollars. Ces fonds sont-ils administrés par Roldugin pour le compte de Poutine ? L'ICIJ n'apporte pas de réponses, mais pose ouvertement la question.

Indice supplémentaire de la communauté de vues, sinon d'intérêts, entre Moscou et WikiLeaks, Julian Assange et Vladimir Poutine réagissent tous les deux violemment à la publication des Panama Papers. Les deux hommes accusent l'organisation d'être le relais d'une opération de propagande américaine. À l'appui de leurs dires, Assange et Poutine soulignent que l'ICIJ compte parmi ses financiers l'agence de développement américaine USAID, équivalent de l'AFD en France et partie intégrante de la diplomatie américaine, mais également le milliardaire américain d'origine hongroise George Soros, célèbre pour l'aide financière qu'il apporte aux mouvements démocratiques en Europe centrale et régulièrement dénoncé par Moscou comme un faux-nez de la CIA. Ironie de l'histoire, c'est précisément auprès de George Soros que, dix ans plus tôt, Assange avait imaginé lever les financements nécessaires pour lancer WikiLeaks… En 2006, Assange avait évoqué avec son partenaire américain John Young, fondateur du site Cryptome, le précurseur de WikiLeaks, la possibilité de demander « cinq millions de dollars à Soros ». L'idée avait hérissé Young et précipité la rupture entre les deux hommes…

Il existe un autre lien entre l'ICIJ et le gouvernement américain : parmi les administrateurs du Center for Public Integrity, maison-mère de l'ICIJ, on trouve Richard M. Lobo, qui a dirigé de 2010 à 2013 l'International Broadcasting Bureau, une branche discrète de la diplomatie américaine qui coordonne toutes les opérations de propagande de Washington, et notamment les radios Voice of America, Radio Free Cuba et Radio Free Europe. La présence de Richard M. Lobo suffit-elle à assimiler l'ICIJ à un relais de la diplomatie américaine ? L'argument, là encore, peut paraître insuffisant : l'International Broadcasting Bureau a largement financé le réseau Internet anonyme Tor, cela afin de permettre aux activistes iraniens et nord-coréens de dialoguer à l'abri de leur gouvernement, mais également de communiquer avec l'extérieur. Or l'un des utilisateurs invétérés de Tor, on l'a vu, n'est autre que… WikiLeaks ! Si les insinuations d'Assange et de Poutine contre l'ICIJ s'avèrent simplificatrices, voire de mauvaise foi, elles touchent néanmoins juste : l'organisation mise en place par Chuck Lewis n'est pas complètement indépendante de la diplomatie américaine et a des liens avec plusieurs administrations chargées de défendre, voire d'avancer les intérêts des États-Unis par la diffusion d'informations. Pour le Kremlin, l'affaire est entendue : les Panama Papers sont une manipulation des

services secrets américains. Dans leur formidable enquête *The Red Web*, déjà citée, Andreï Soldatov et Irina Borogan révèlent même que c'est à la suite de cette fuite massive que les dirigeants russes décideront de répliquer en piratant les messageries du Parti démocrate…

Pour éviter de susciter ce genre de réactions, les consortiums de journalistes qui, après l'ICIJ, se mettront en place pour traiter des fuites massives adoptent une attitude beaucoup plus distante vis-à-vis des institutions gouvernementales et privées. L'European Investigative Collaborations, par exemple, ne reçoit aucun financement d'État.

Tout en critiquant l'ICIJ, Julian Assange s'est inspiré des méthodes de l'organisation : à partir de 2012, WikiLeaks opère une imperceptible transformation, se muant en plateforme de services relayant des fuites massives dont elle n'est pas, à l'origine, destinataire. L'organisation de Julian Assange publie successivement les e-mails internes à l'entreprise d'interception italienne Hacking Team, apparus, on l'a vu, sur un site éphémère, puis des télégrammes diplomatiques saoudiens et enfin la messagerie de la campagne d'Emmanuel Macron. Chaque fois, comme l'a fait l'ICIJ pour les Panama Papers, WikiLeaks enrichit ces bases de données d'un moteur de recherche performant et d'un système d'indexation destiné à faciliter les consultations. Ce recyclage permet à WikiLeaks de rester présent sur le marché de la fuite et de ne pas se laisser complètement doubler par l'ICIJ.

*

Les diatribes de Vladimir Poutine contre l'ICIJ participent d'une chorégraphie bien réglée : chaque nouvelle fuite massive suscite des accusations de manipulation, mais uniquement de la part du pays ou de l'entreprise qui est visé. Jamais aucun média ni, *a fortiori*, aucune plate-forme de diffusion de fuites type WikiLeaks, n'informe ses lecteurs sur les coulisses de l'opération, le circuit suivi par les informations reçues et les éventuelles motivations des individus qui ont transmis les données. Au nom de la protection des sources, un mur inviolable est systématiquement érigé entre les documents divulgués et leur origine.

Cette omerta suscite une frustration croissante dans les pays déstabilisés par des fuites, notamment dans l'administration américaine, cible quasi

exclusive de WikiLeaks, mais également des révélations d'Edward Snowden. Invité le 30 mars 2017 à témoigner devant la Commission du renseignement du Sénat américain, l'universitaire britannique Thomas Rid, spécialiste des questions de stratégie au King's College de Londres, résumera la pensée de nombreux responsables américains en déclarant :

> Parmi les agents inconscients [des opérations de déstabilisation russes envers les États-Unis], on trouve les journalistes qui ont activement couvert les fuites massives tout en négligeant ou ignorant leur origine. Avec une très grande habileté, le bloc soviétique à l'époque [de la guerre froide] a fourni plusieurs centaines des documents altérés, ou bien soigneusement sélectionnés, à des journalistes. Mais de telles opérations nécessitaient un savoir-faire : fabriquer des documents, susciter la confiance, scénariser l'apparition des pièces. À l'époque de la guerre froide, la désinformation était artisanale : aujourd'hui, elle est en partie sous-traitée à la victime elle-même. Les journalistes américains fouillent dans les masses de documents qui leur sont fournies et, tout en extrayant des informations, ils maximisent l'impact d'une opération.

Éclaboussé par la fuite massive qui a visé Sony en 2014 (voir chapitre 3), le scénariste Aaron Sorkin, fin connaisseur des arcanes de Washington, auxquelles il a consacré une série à succès (*À la Maison-Blanche*), ne dit pas autre chose quand il signe en décembre 2014 dans le *New York Times* un éditorial intitulé « La presse ne devrait pas aider les hackers ».

> Je comprends que les médias aient régulièrement recours à de l'information volée, écrit Sorkin. C'est de cette manière, comme on le répète souvent, que sont apparus les Pentagon Papers [qui révélaient les nombreuses exactions commises par l'armée américaine au Vietnam]. Mais il n'y a aucune information [dans les e-mails internes à Sony] dont l'intérêt puisse être comparé, même de manière lointaine, avec les informations contenues dans les Pentagon Papers. Est-ce que ces e-mails montrent que Sony enfreignait la loi ? Non. Que l'entreprise trompait le public ? Non. Qu'elle agissait en contravention directe avec le bien-être des consommateurs, comme les fabricants de tabac ou Enron ? Non. Est-ce qu'il y a ne serait-ce qu'une phrase dans l'un de ces e-mails volés qui pourrait indiquer un méfait ? Quelque chose qui pourrait aider, informer ou protéger quelqu'un ? […] Je sais, poursuit

> Sorkin, qu'il y a des détails croustillants dans ces e-mails et je sais que certains d'entre nous y sont insultés. Aucune vie privée ne sort indemne d'un examen public. Mais il s'agit ici de quelque chose de plus important que des vexations et des ego humiliés. Fermez les yeux et imaginez les hackers [qui ont piraté les messageries de Sony] assis dans une pièce et examinant les documents pour trouver celui qui fera le plus mal. Et dans une autre pièce, les journalistes, qui font exactement la même chose. Aussi dément, voire criminel que cela puisse sembler, les hackers, eux, agissent pour une cause. Les journalistes, eux, le font pour augmenter leurs ventes.

Il ne s'agit pas, encore une fois, de distribuer les bons et les mauvais points. Nous avons trop lu les bandes dessinées d'Hugo Pratt pour ne pas reprendre à notre compte les propos de son héros, Corto Maltese : « Qui suis-je pour juger ? Mais j'ai une antipathie innée pour les censeurs, les prud'hommes et, par-dessus tout, pour les rédempteurs. » Mais force est de constater que les propos de Rid et de Sorkin, si violents soient-ils, comportent une part de vérité : les journalistes, nous les premiers, n'ont pas toujours été suffisamment vigilants sur les motivations des fuites massives qu'ils ont relayées et se sont parfois rendus involontairement complices d'opérations dont l'enjeu dépassait largement la valeur des informations qu'ils publiaient.

Après dix ans de fuites massives, une sorte de prise de conscience fait peu à peu son chemin dans les médias. En décembre 2016, lorsqu'il révèle les documents internes au fonds d'investissement sportif Doyen sous le nom de Football Leaks (voir chapitre 5), l'European Investigative Collaborations (EIC) lancé par *Der Spiegel* expose, pour la première fois, ses doutes : « Les médias partenaires de l'European Investigative Collaborations ont choisi de publier des articles basés sur les documents de Football Leaks bien que nous n'ayons pas pu déterminer qui se trouve réellement derrière ce projet. » Mieux, les journaux associés à l'opération reconnaissent, dans un texte commun, que la fuite massive dont ils ont bénéficié est probablement issue d'un piratage et racontent même que les présumés pirates ont d'abord tenté de faire chanter Doyen avant de leur communiquer les informations.

Mais c'est la fuite des messageries internes à la campagne d'Emmanuel Macron qui change véritablement la donne. Diffusés le 6 mai 2017, à deux

jours du second tour de l'élection présidentielle française, les documents ne sont pas tout de suite exploités par la presse, contrairement aux e-mails du Parti démocrate publiés par WikiLeaks neuf mois plus tôt. Les premiers articles consacrés à la fuite se contenteront de souligner que les e-mails ont été manifestement piratés et que leur diffusion a été largement relayée par des militants d'extrême droite américains. La raison de ce silence n'est pas uniquement vertueuse : le parti du futur nouveau président français a bombardé les rédactions d'injonctions judiciaires pour éviter tout article. La Lettre A, première publication à utiliser ces données pour contacter les donateurs de la campagne d'Emmanuel Macron et publier les noms de ceux qui lui ont confirmé leurs contributions, sera frappée d'une plainte pour « recel d'accès frauduleux à des données de masse » dès l'entrée en fonction du nouveau président (La Lettre A est publiée par Indigo Publications, dont l'un d'entre nous dirige la rédaction et qui publie également Intelligence Online).

Cette retenue – largement contrainte, mais malgré tout réelle – suscitera l'étonnement des médias américains : interviewé par le *Washington Post* le 8 mai, Jérôme Fenoglio, le directeur du quotidien *Le Monde*, ne se privera pas de leur faire la leçon, expliquant notamment que la réaction des médias français devrait être un exemple pour les journalistes du monde entier, y compris pour les américains, coupables de s'être précipités pour diffuser les fuites pré-électorales sans enquêter sur leur origine. Un plaidoyer de circonstance : *Le Monde* s'est battu pour participer à toutes les principales fuites massives des dix dernières années et n'a jamais particulièrement brillé par sa pugnacité à élucider l'origine des fuites qu'il relayait, allant même jusqu'à publier une lettre ouverte du fondateur de WikiLeaks demandant que la France lui accorde l'asile politique… La mise en garde, malgré tout, sera entendue.

L'épisode Macron Leaks a également pour conséquence de creuser un peu plus le fossé entre la presse et WikiLeaks. À rebours des journaux français, le site de Julian Assange publie en juillet 2017 l'intégralité des mails piratés de la campagne d'Emmanuel Macron. Et fait désormais cavalier seul : en avril 2017, lorsque WikiLeaks diffuse une série de logiciels utilisés par la CIA pour intercepter des flux de communication électronique, l'organisation procède sans s'associer à aucun média et assure

elle-même l'analyse des informations révélées. Les commentaires étant anonymes et, pour la plupart, non sourcés, ils suscitent des raccourcis simplificateurs chez les lecteurs, obligeant de nombreux médias (y compris notre lettre d'information Intelligence Online) à rappeler que la CIA, contrairement à son homologue la NSA, ne mène que des cyberopérations sur des individus ou des groupuscules, et non une surveillance mondiale et indiscriminée.

* * *

Encore une fois, c'est la guerre froide qui s'impose comme la grille de lecture la plus pertinente pour comprendre les méthodes à l'œuvre dans les fuites massives de données, et singulièrement le rôle qu'y jouent les médias. Dans son livre *The KGB and Soviet Disinformation*, le transfuge tchèque Ladislav Bittman cite une phrase du général russe Ivan Agayants, grand maître soviétique de la manipulation médiatique : « S'il [l'Occident] n'avait pas la liberté de la presse, il faudrait l'inventer. »

Durant les années 1960 et 1970, le service de renseignement russe a en effet activement ciblé les médias progressistes européens pour faire avancer ses intérêts, tout comme la CIA a, de son côté, régulièrement manipulé la presse conservatrice. Un épisode nous semble particulièrement riche d'enseignement pour la situation présente : celui de Philip Agee. Agent de la CIA en poste en Équateur, en Uruguay et au Mexique, Agee a quitté avec fracas le service de renseignement américain en 1968 pour se réfugier à Londres et devenir journaliste. Son premier livre, *Inside the Company*, est un récit circonstancié de sa carrière d'agent secret, assorti d'un index de 250 noms de responsables de la CIA opérant sous couverture. Agee a ensuite publié deux autres volumes exposant l'identité de presque tous les fonctionnaires du renseignement américain en poste en Europe et en Afrique, et lancé, en 1978, un magazine spécialisé, *Covert Action Quaterly*, qui chroniquait avec une précision parfois sidérante les activités de la CIA dans le monde. La quasi-totalité des informations révélées par Agee étaient vraies et, pour l'essentiel, très dommageables pour la CIA, qui a été contrainte de rappeler de nombreux agents et d'arrêter des opérations en cours. Très progressiste, Agee justifiait ses attaques contre son ancien

employeur par les liens qui unissaient la CIA aux régimes autoritaires d'Amérique du Sud et d'Afrique, la rendant complice de nombreuses exactions. En représailles, l'agence américaine a pourchassé Agee toute sa vie et l'a fait déporter de nombreux pays européens – Royaume-Uni, France, Pays-Bas. Au milieu des années 1980, Oleg Kalugin, ancien responsable du contre-espionnage du KGB, fit défection aux États-Unis et révéla qu'Agee était épaulé, sinon activement dirigé, par les services de renseignement cubains et donc, indirectement, par le KGB. Agee a fini sa vie à Cuba, seul pays qui ait accepté de braver l'interdit américain à son encontre, et est mort à La Havane en 2008.

À près de cinquante ans de distance, on retrouve des similitudes frappantes entre les trajectoires de Julian Assange et d'Edward Snowden et celle de Philip Agee. Les techniques de manipulation de l'information qui firent florès dans les années 1960 et 1970 se sont perfectionnées et ont changé d'échelle, pour devenir massives, globales et instantanées.

VII

Les profiteurs

Perpétuellement menacés par une fuite massive de données, les États et les entreprises tentent désespérément de trouver la parade. Tout est bon pour ne plus voir ses secrets exposés sur Internet… La peur panique du piratage a suscité un marché dérivé, celui de la prévention des fuites. Des cabinets privés vendent à prix d'or toute une gamme de contre-mesures censées décourager les hackers. Ces sociétés sont le plus souvent dirigées par des anciens du renseignement, dont beaucoup sont issus des unités cyber. Mais d'autres plombiers de la fuite massive ont, eux, reçu une formation en renseignement humain. Reconvertis dans le privé, ces psychanalystes de la faille réseau travaillent à identifier les défaillances humaines qui facilitent les piratages massifs. Leurs clients ? Les multinationales, notamment financières, mais également les ministères et les administrations, inquiets de voir leurs informations les plus sensibles exposées sur Internet.

Les premières diffusions de bases de données confidentielles ont donné lieu à des contre-attaques très agressives qui, toutes, se sont soldées par des échecs, parfois humiliants. Petit à petit, les chasseurs de fuites ont perfectionné leurs méthodes. Certains cabinets scannent à longueur de journée Internet et son pendant invisible, le Darknet, à la recherche d'un hack en cours ou de données confidentielles à racheter pour éviter leur diffusion. Mais d'autres petites boutiques proposent à leurs clients de traquer le prochain Edward Snowden et mettent en place des programmes de surveillance d'employés et de fonctionnaires, veillant à ce que ceux-ci ne soient pas tentés de communiquer des données confidentielles à l'extérieur… Plongée dans la contre-attaque mondiale contre les fuites massives.

*

Après les premières fuites orchestrées par WikiLeaks en 2010 contre le Pentagone et le Département d'État, Washington a d'abord cherché à contre-attaquer en se servant des mêmes outils que l'organisation de Julian Assange.

À la fin de l'année 2010, un consultant privé, HBGary Federal, a ainsi voulu monter une véritable campagne de contre-insurrection pour endiguer WikiLeaks. Filiale du géant de la sécurité informatique HBGary Inc., HBGary Federal était spécialisé dans les cyberenquêtes pour le compte d'agences et d'administrations américaines. Le cabinet développait en parallèle des logiciels malveillants capables de pénétrer des réseaux informatiques que le renseignement américain souhaitait infiltrer. HBGary Federal avait même songé à créer et opérer un réseau de faux profils sur les réseaux sociaux pour le compte du gouvernement américain, cela afin de mener des opérations d'influence clandestines, comme le fera plus tard la Russie.

À partir de la mi-2010, le patron de HBGary Federal, Aaron Barr, un spécialiste de la cybersécurité, se met en tête d'identifier les leaders de l'organisation de hackers Anonymous, alors très proche de WikiLeaks. Grâce à une étude fine des réseaux sociaux (Facebook, Twitter, etc.), complétée par de multiples tentatives d'infiltration des forums utilisés par Anonymous, il veut démasquer ce collectif de pirates, qui a mené plusieurs fuites massives de données. Mais Barr fait l'erreur de faire publiquement état de son enquête et annonce qu'il diffusera les noms des principales figures d'Anonymous… Une initiative pour le moins malheureuse : les chasseurs de pirates opèrent généralement dans l'ombre. Mais HBGary Federal traverse alors une mauvaise passe et a besoin de publicité.

Les rodomontades d'Aaron Barr ne passent pas inaperçues, et Anonymous ne tarde pas à réagir. Au début de l'année 2011, quelques semaines après les annonces tonitruantes du patron de HBGary Federal, le collectif de hackers pénètre les réseaux de la société, subtilisant plusieurs dizaines de milliers de documents internes. Les pirates sont entrés sans encombre par les brèches du logiciel de gestion du site, créé sur mesure, mais mal protégé. Pour une société qui fabrique des virus et des logiciels de pénétration, se faire pirater de la sorte est une humiliation dont on se relève difficilement…

Les documents piratés, et diligemment publiés par les hackers, révèlent que l'enquête de HBGary sur Anonymous était en réalité une commande du principal établissement financier des États-Unis, Bank of America (BoA). À la fin de l'année 2010, Julian Assange avait annoncé à plusieurs reprises qu'il préparait la mise en ligne d'un stock massif de documents internes à BoA. Paniquée, la direction de la banque avait mandaté HBGary pour tenter d'éviter le désastre annoncé. Pour mener à bien cette mission de contre-insurrection, la société a mis en place un véritable corps expéditionnaire contre WikiLeaks. Ainsi, Palantir Technologies et Berico Technologies, prestataires réguliers de la communauté américaine du renseignement, ont rejoint HBGary au sein d'un projet d'alliance visant à déstabiliser WikiLeaks. Cette conjuration, baptisée Team Themis dans les documents de HBGary, aurait eu pour vocation de transmettre de faux documents à l'organisation, afin de la compromettre et de ruiner sa réputation. L'impact d'une fuite réside avant tout dans la véracité des documents publiés, et le bilan de WikiLeaks, sur ce sujet, est irréprochable : toutes les données publiées par l'organisation sont authentiques. Le piège imaginé par la coalition de consultants aurait pu détruire en quelques heures la réputation de Julian Assange.

Mais la Team Themis fomentait d'autres projets : les cyberconjurés avaient notamment prévu de monter une opération clandestine pour pénétrer les serveurs de WikiLeaks et démasquer les administrateurs du site, qui sont anonymes. Ils avaient même songé, comme le faisait le FBI dans les années 1960, à compromettre quelques apôtres de la fuite de données, notamment l'éditorialiste américain Glenn Greenwald. Avocat reconverti dans la presse Internet et militant de la transparence, Greenwald dispose alors d'une chronique sur le site Internet du *Guardian*, où il défend l'action de WikiLeaks et des Anonymous. En 2013, c'est à lui qu'Edward Snowden remettra les millions de documents qu'il a subtilisés à la NSA.

Mais tous ces projets de contre-subversion électronique sont tués dans l'œuf par la publication des e-mails internes de HBGary Federal. Aaron Barr, le PDG, est contraint à la démission dans les jours qui suivent. La direction de Palantir, l'une des sociétés associées à HBGary sur ce projet, s'excuse personnellement auprès de Glenn Greenwald pour avoir participé à la conjuration et coupe tout contact avec Barr. HBGary Federal met rapidement la clé sous la porte, tandis que la maison-mère, HBGary Inc., est

vendue à une autre société de cybersécurité, Mantech International, l'année suivante.

Le 29 novembre 2016, WikiLeaks met en ligne tous les e-mails volés sur les serveurs de HBGary. Cette publication est prévue pour coïncider avec la sortie de prison de Barrett Brown, le hacker et journaliste qui avait écrit les premiers articles sur le piratage de la société. Arrêté par le FBI, puis emprisonné en 2012, Brown a été accusé d'une trop grande proximité avec ses sources. Familier des Anonymous, qu'il fréquente depuis de nombreuses années, il aurait directement participé au piratage des données de HBGary, mais également de la société de renseignement stratégique Stratfor. Il a plaidé coupable.

Après ce fiasco embarrassant, dont la seule conséquence a été de donner une légitimité accrue aux diffuseurs de fuites, les sociétés de sécurité informatique se sont positionnées nettement plus en amont de la chaîne des opérations de *hacking-and-leaking*, comme les qualifie le chercheur britannique Thomas Rid.

*

Après avoir vainement tenté de s'en prendre directement aux plateformes de diffusion de fuites massives comme WikiLeaks, les consultants ont proposé à leurs clients de prévenir les fuites massives de données en intervenant directement là où elles sont planifiées et négociées, sur le Darknet. Cette zone non référencé d'Internet, uniquement constituée de forums d'initiés, héberge plus d'activité que l'Internet visible. Tout s'y échange, depuis le balluchon de cocaïne jusqu'à la caisse de kalachnikovs, en passant par les dernières innovations pornographiques. C'est aussi là que se retrouvent les hackers de toutes les nationalités. Si l'anglais prédomine comme langue vernaculaire, force est de constater que le cyrillique et le mandarin occupent une place prépondérante sur les listes de discussions clandestines.

Via des protocoles d'anonymisation, les génies de la pénétration informatique échangent et se revendent les dernières lignes de codes en vogue et surtout les failles *zero-day*, ces erreurs de programmation que les fabricants de logiciels n'ont pas encore détectées et qui facilitent les intrusions. Les montants négociés pour acquérir ces portes informatiques

dérobées peuvent s'avérer substantiels, surtout si elles ont été testées et sont donc opérationnelles. C'est aussi sur le Darknet que se commanditent les piratages de masse. Les paiements s'effectuent en monnaie cryptée bitcoin, les plus prudents utilisant systématiquement des comptes-séquestres, où les fonds ne sont débloqués qu'une fois la prestation effectuée.

Dans cet espace, tout le monde opère à couvert, sous une identité virtuelle appelée « avatar ». Plus un pseudonyme est connu et reconnu dans le sous-monde du Darknet, plus les autres participants vont lui faire confiance. Sans un avatar crédible, rien n'est accessible sur l'Internet clandestin, tant la paranoïa est aiguë. Non sans raison : les plus grands services de renseignement de la planète sont tous actifs, sous couverture, sur le Darknet.

Le FBI, la police fédérale américaine, dispose ainsi d'une unité uniquement affectée à la surveillance des bas-fonds d'Internet. Tous ces services étatiques opèrent de manière similaire aux hackers, c'est-à-dire sous couvert d'avatars, ces sortes d'identités fictives virtuelles, de cyberlégendes. Depuis les dernières lois françaises sur le renseignement de 2015, les agents de la plupart des services français sont autorisés à créer, et à opérer sous de fausses identités en ligne, de même que les enquêteurs des douanes qui auscultent les réseaux de trafiquants en tout genre qui pullulent sur le Darknet.

Grâce à un contact à Tel Aviv, nous avons pu mener une incursion sous couverture dans cette zone de non-droit. Notre avatar était une couverture bien établie, un profil rodé pendant des années sur les forums clandestins les plus hostiles. Cette identité virtuelle datait de plusieurs années, sinon une décennie, et était identifiée comme fiable par les usagers du Darknet. Aucun des intervenants sur les forums de piratage ne se doutait que derrière cet avatar se cachait un ancien du renseignement technique israélien, qui les avait infiltrés depuis belle lurette. Pour la démonstration, un grand écran LCD était installé sur le mur d'une petite salle anonyme, dont les stores étaient tous baissés. Sur le forum où nous avions pénétré s'affichaient toutes les failles informatiques d'une grande entreprise, cliente de notre contact, en particulier tous ses sous-traitants. Pour les hackers, cibler les prestataires d'une multinationale est souvent le moyen le plus sûr de contourner les dispositifs de sécurité : comme nous l'a confié notre guide, « les consultants

extérieurs disposent de tous les accès aux réseaux de leurs clients, mais protègent mal leurs propres systèmes ».

Pénétrant plus avant dans les listes de discussions consacrées au piratage, notre sherpa, se servant d'algorithmes de recherche adaptés à cet environnement, traque tous les échanges pouvant avoir trait à son client, qu'il s'agisse de localiser ses failles de sécurité ou bien de vendre des données qui lui auraient été illégalement subtilisées. Si une telle menace est effectivement détectée, l'ancien cyberespion israélien peut interagir directement avec les contributeurs du forum, voire racheter les documents piratés à son client, comme le ferait un négociateur spécialisé dans la libération d'otages.

Aujourd'hui, les plus grandes sociétés mondiales ont toutes des consultants qui surveillent le Darknet au jour le jour, afin de détecter la moindres cybermenace : un hacker en quête de failles *zero-day* de son système informatique ; des données volées sur son intranet qui circuleraient sur un forum et pourraient être utilisées par des maîtres chanteurs ; des fichiers-clients entiers abandonnés aux quatre vents du Darknet… Autant de menaces scrutées de près par ces consultants masqués.

Sur ce secteur de niche, les plus efficaces sont ceux qui ont déjà un pied dans le Darknet, qu'ils ont pénétré lorsqu'ils étaient fonctionnaires d'un service de renseignement. Présentes sur le Darknet depuis l'émergence de cette plateforme et disposant d'avatars rodés par des années de pratique, les sociétés israéliennes dominent ce marché de l'infiltration des forums clandestins et comptent aujourd'hui dans leur portefeuille de clients tout Wall Street et, bien souvent, de grands noms de la Silicon Valley. Très exposé aux menaces de fuites de données, le secteur bancaire et financier est en effet le principal consommateur de ces services de surveillance sous couverture. Un fichier bancaire qui fuite et c'est toute la confiance des clients dans la sécurité de l'établissement qui est durablement ébranlée.

Outre les vols de données, les cybermercenaires du Darknet traquent également des complots qui n'ont rien de virtuel. À la suite des pirates et des trafiquants, les militants radicaux, voire djihadistes, utilisent de plus en plus le Darknet pour planifier des actions. Pour prévenir toute attaque sur les Jeux olympiques de 2016, les autorités brésiliennes avaient mandaté la société israélienne Kela Intelligence pour surveiller le Darknet pendant les épreuves et détecter d'éventuelles préparations d'attentats.

Cette surveillance tous azimuts a un prix. Les authentiques cyberopposants en lutte contre les régimes autoritaires ne peuvent plus compter sur le Darknet pour mobiliser des sympathisants et trouver des soutiens. Des bataillons entiers du cyberrenseignement chinois ou russe, par exemple, sont présents sur les forums clandestins et scrutent en permanence les échanges entre activistes.

Utile pour détecter une attaque de hackers sur les réseaux d'une entreprise, la surveillance du Darknet est en revanche totalement inefficace pour empêcher un employé de voler des données à son employeur. Aux côtés des vengeurs masqués du Darknet, d'autres sociétés se sont spécialisées dans la prévention des fuites internes.

*

Pour parer aux fuites massives de données, un nouveau marché se met petit à petit en place, particulièrement aux États-Unis. Il s'agit de traquer les menaces internes (*insider threats*) à une organisation, c'est-à-dire débusquer, en utilisant les méthodes éprouvées du contre-espionnage, les employés et les sous-traitants susceptibles d'être déloyaux envers leur employeur et de communiquer, soit par frustration professionnelle, soit par conviction personnelle, des données confidentielles à l'extérieur de l'entreprise. Dans ce schéma, chaque salarié, chaque fonctionnaire devient une menace potentielle pour l'organisation qui l'emploie. Ambiance garantie en interne…

Qu'ils interviennent dans des secteurs stratégiques (défense, soutien au renseignement, énergie, etc.) ou dans des domaines où l'information et la propriété intellectuelle sont l'alpha et l'oméga (divertissement, luxe, pharmacie, etc.), les grands groupes américains ont tous mis en place des programmes de surveillance de leur masse salariale. Pour les sociétés qui vendent ce type de services, la mesure de la menace est le meilleur argument marketing : le géant des télécoms Verizon produit régulièrement une étude, baptisée Data Breach Investigations Report, qui montre que les vols de données internes seraient en forte progression. Qu'elle soit réelle ou fantasmée, cette augmentation des cas de fuites imputables à des salariés est principalement due, selon plusieurs chasseurs engagés dans cette traque, à l'explosion des moyens anonymes et sécurisés de communication. En

passant par des messageries chiffrées comme WhatsApp et d'autres, l'employé mécontent peut se venger de son employeur en toute sécurité. Cette évolution des moyens fait dire à un dirigeant d'une des principales sociétés du secteur que « chaque employé, utilisateur, sous-traitant, partenaire est aujourd'hui une menace d'importance pour toute organisation ». Si orwellien soit-il, cet état d'esprit est en train de gagner toutes les grandes compagnies américaines et les institutions sensibles du pays.

Une paranoïa qui fait les choux gras de quelques entrepreneurs habiles, surfant sur le vent de panique qui souffle au sein des conseils d'administration. La première entreprise à avoir flairé le bon filon se nomme Cognitio. Fondée par de grands pontes des principaux services américains de renseignement, elle est présidée par Roger Hockenberry, l'ancien directeur technique du National Clandestine Service (NCS) de la CIA. Le NCS est la pépite cachée de l'agence de Langley : c'est cette unité d'élite qui pilote tous les agents sous couverture de la CIA dans le monde. Le directeur technique du NCS a la délicate tâche de cyberprotéger ces espions clandestins, mais également de leur fournir une identité virtuelle solide, ainsi que les cyberoutils nécessaires à leurs missions (virus, porte dérobée pour s'introduire dans un système informatique, etc.). Car si la National Security Agency (NSA), la principale agence d'interception électronique américaine, surveille massivement les réseaux de communication, la CIA peut également mener des cybermissions de pointe, plus ponctuelles et ciblées. Au sein de Cognitio, Hockenberry est d'ailleurs entouré de Bob Flores, l'ancien directeur technique de toute l'agence, précisément en charge de superviser la création et le développement des virus informatiques utilisés par les agents de Langley. Certains de ces logiciels ont été dévoilés par WikiLeaks à partir de mars 2017, dans une série de documents que le site a appelés *Vault 7*. Ceux-ci montrent comment la CIA peut, dans le cadre d'opérations très ciblées contre un individu, pénétrer des systèmes d'exploitation de Google, d'Apple, mais également transformer des téléviseurs connectés en micros, à l'aide de programmes insérés dans des clés USB. Surtout, ces documents révèlent que la direction technique de l'agence, via le *malware* Marble, peut camoufler ses traces et insérer des fragments de code en d'autres langues (chinois, russe, arabe, farsi) afin d'attribuer une attaque à un autre État, complexifiant d'autant les enquêtes d'attribution dans le cybermonde…

Outre Cognitio, le cabinet Big Sky Associates s'est également imposé sur le marché de la surveillance de fonctionnaires et de salariés. Dirigé par un vétéran de la CIA, John Millard, associé à l'ancien commandant de l'US Army Cyberdefense Directorate, Steven Smith, Big Sky est déjà l'un des prestataires privilégiés de l'Office of the Director of National Intelligence (ODNI), le coordinateur de toutes les agences de renseignement des États-Unis. La mission de Big Sky ? Détecter d'éventuels « ennemis de l'intérieur » au sein des services, qu'ils soient djihadistes, militants ou agents doubles… Big Sky a même participé à la toute première revue stratégique du Pentagone, en 2009, qui, déjà, visait à détecter les menaces internes, notamment les militaires aux sympathies djihadistes. Ce travail faisait suite à l'assassinat de treize soldats sur la base texane de Fort Hood par un psychiatre militaire, Nidal Malik Hassan. La société n'a eu qu'à élargir son spectre de menaces internes aux agents susceptibles de transmettre des informations à WikiLeaks…

Car, outre le secteur privé, ces contre-espions de la fuite massive disposent également de contrats avec les administrations publiques américaines, véritables passoires informationnelles. Depuis l'affaire Snowden, on pensait la communauté du renseignement américain immunisée et préparée contre de telles fuites. Mais la divulgation par WikiLeaks, au début de 2017, de toute la gamme des virus et logiciels malveillants utilisés par la NSA et la CIA, montre que les services américains de renseignement restent incapables de juguler les fuites d'informations privilégiées. Les révélations de WikiLeaks, auxquelles l'organisation a donné le nom de *Vault 7*, visaient tout particulièrement la CIA, jusqu'ici épargnée par le phénomène des fuites massives. Les documents auraient été obtenus auprès d'un sous-traitant de l'agence, un scénario identique à la fuite qui a frappé la NSA, trahie par son consultant, Edward Snowden, lequel a copié une partie de la base de données du service d'interception et a confié les documents subtilisés à plusieurs médias internationaux…

Autrement dit, cinq ans après avoir été mis à genoux par l'un de ses propres administrateurs réseau, le gouvernement américain n'a pas résolu ses problèmes de sécurité informatique. Dans la frénésie de l'après-11 septembre 2001, plusieurs millions d'Américains se sont vu attribuer des accréditations secret-défense pour travailler dans les unités antiterroristes. D'un coup, ces nouvelles recrues ont eu accès aux informations les plus

sensibles du pays, sans que les contrôles internes soient renforcés : la priorité était alors l'efficacité – on était obsédé par tout ce qui pouvait retarder l'identification d'un projet terroriste rejeté comme « trop bureaucratique ». En 2014, on estimait qu'un peu plus de cinq millions d'Américains étaient accrédités « secret-défense », soit 1,5 % de la population active, l'un des taux les plus élevés au monde. Comme le note le chercheur de l'université de Stanford Scott Sagan, qui a beaucoup travaillé sur les menaces internes au sein de l'appareil de sécurité américain, « il y a une tendance malheureuse, au fur et à mesure des fuites massives de données ou des cas d'espionnage avérés, qui est de classifier encore plus d'informations au nom de l'amélioration de la sécurité nationale. Mais cela peut se retourner contre elle-même, car plus les informations sont classifiées, plus nombreux sont les individus qui ont besoin d'accréditation, et moins les contrôles de sécurité sont bien appliqués du fait du nombre ». Un cercle vicieux qui se retourne contre la toute-puissance du renseignement américain.

Le contrôle de ces accréditations, ainsi que les enquêtes de sécurité sur les individus qui les sollicitent – criblage de l'environnement des demandeurs, vérification de leur CV, profilage psychologique –, est théoriquement effectué par un organe gouvernemental, l'Office of Personnel Management (OPM). Mais, submergé par la tâche et ne disposant pas d'équipes suffisantes, cette administration sous-traite les investigations de routine à des opérateurs privés, qui privilégient le volume des enquêtes réalisées au détriment de leur précision. Résultat, l'OPM a dû à plusieurs reprises se retourner en justice contre ses propres prestataires, notamment contre une société appelée USIS, accusée d'avoir bâclé des centaines de milliers d'enquêtes de sécurité, dont celle d'Edward Snowden…

Plusieurs agences de renseignement américaines ont déjà discrètement émis des appels d'offres réservés aux opérateurs de contre-espionnage privés pour leur confier la traque des futurs Chelsea Manning et Edward Snowden. Big Sky Associates conseille déjà l'une des principales agences du renseignement des États-Unis, la National Geospatial-Intelligence Agency (NGA), qui gère la flotte de satellites espions en orbite autour du globe. Selon nos informations, Cognitio a quant à elle déjà fait à plusieurs reprises des présentations commerciales aux pontes de la Defense Intelligence Agency (DIA), l'agence américaine de renseignement militaire, pour vendre ses services. Surtout, ces sociétés se sont ces derniers mois

positionnées pour décrocher un méga-budget de l'Intelligence Advanced Research Projects Activity (IARPA), le laboratoire de recherche du renseignement américain. L'IARPA a en effet lancé un tout nouveau programme ultrasecret dans ce domaine, baptisé Scientific Advances to Continuous Insider Threat Evaluation (SCITE), qui cherche à calculer et à réduire la probabilité de fuites massives ainsi que le degré de menace que constitue chaque agent du gouvernement américain. Outre surveiller le trafic informatique, SCITE veut également prendre en compte des facteurs plus privés et humains, comme des revenus non déclarés, des désaccords avec la hiérarchie, etc. À côté du tentaculaire appareil de renseignement américain se met ainsi en place, dans une course technologique effrénée, une administration-miroir, dont le seul but est de surveiller les surveillants… Mais qu'arrivera-t-il quand ces cybervigies seront elles-mêmes victimes d'une fuite massive ?

Arme parfaitement calibrée pour l'époque de l'information-reine et de l'interconnexion permanente, la fuite massive est aussi facile à mettre en place qu'elle est complexe à prévoir et presque impossible à contrer. Même dotés d'un véritable arsenal informatique, les consultants qui garantissent la sécurité informatique absolue vendent plus souvent du rêve que des programmes efficaces et se contentent de prospérer sur une paranoïa aussi diffuse que tenace.

Épilogue

Au commencement étaient Bradley Manning, Antoine Deltour et quelques autres, une poignée d'individus perdus dans des organisations gigantesques et cherchant à dénoncer les abus dont ils étaient les témoins. Pour gripper ces systèmes trop grands pour eux, ils ont rendu publics des giga-octets de documents confidentiels en utilisant des logiciels de cryptage et de transfert de données. Mais ces armes du pauvre sont presque instantanément passées des mains des activistes à celles des puissances qu'ils combattent et, comme a tenté de le montrer notre enquête, sont aujourd'hui plus souvent utilisées par les États, les multinationales et les grandes fortunes pour régler leurs comptes que par des individus en quête de justice. Dans cette guerre mondiale de la donnée, l'asymétrie reste cependant la règle : les pays et les entreprises qui pratiquent la fuite massive de manière assidue le font parce qu'ils n'ont pas d'autres armes à leur disposition. C'est notamment le cas de la Russie : si elle a épaulé des opérations de déstabilisation numérique contre les États-Unis, c'est parce que Moscou est en infériorité stratégique vis-à-vis de Washington, notamment en matière de technologie d'interceptions.

Du dévoiement de la fuite massive, on pourrait tirer une ribambelle d'analyses politiques et philosophiques : nous laissons ce soin à d'autres. On trouve aujourd'hui des commentateurs à tous les coins de rue, il suffit d'ouvrir le robinet. Notre seul but, dans ce livre, était de raconter de l'intérieur un phénomène aussi contemporain que mal connu.

Une chose nous frappe cependant : la militarisation des données personnelles dont procède la fuisse massive est l'image inversée de l'économie moderne, tout entière centrée sur l'exploitation des identités, des goûts et des parcours des consommateurs. Comme Facebook ou Amazon, dont le succès et la fortune dérivent d'une exploitation méthodique et raisonnée de milliards d'informations individuelles, les tacticiens de la fuite massive sont aussi des prospecteurs de data, des chercheurs de cet or gris que constituent les messages confidentiels et privés. Google, on l'a vu, est le modèle avoué de Julian Assange, le

fondateur de WikiLeaks. Le « Leak » est l'arme du capitalisme de l'information, et la donnée sa matière première, comme l'a été le pétrole pour l'ère industrielle. Depuis cette année, pour la première fois de l'histoire, aux États-Unis, la capitalisation boursière des géants du Big Data est supérieure à celle du secteur pétrolier du pays…

Comment ne pas se transformer en fantassin anonyme dans cette guerre mondiale des data ? C'est une question que nous nous sommes souvent posée en rédigeant ce livre. Nous ne sommes pas, on l'a dit, des informaticiens (l'un d'entre nous pourrait même être décrit comme ignare en la matière). Autrement dit, nous ne connaissons pas le moyen miracle pour protéger ses données. Pour être francs, nous doutons même qu'il existe : si un groupe est déterminé à pirater une messagerie, même très protégée, nous sommes persuadés qu'il parviendra à ses fins. Les systèmes de cryptage type PGP, les messageries instantanées et chiffrées comme WhatsApp sont de bons outils, mais ils ne sont en aucun cas infaillibles.

Mieux : comme nous avons pu le constater au cours de notre enquête, ce ne sont pas les logiciels qui sont le meilleur allié des pirates, mais les comportements humains. Ce sont les employés du Parti démocrate américain qui ont eux-mêmes cliqué sur des liens paramétrés pour susciter leur curiosité, ouvrant leur messagerie aux assaillants masqués. Même constat pour les salariés de Sony, les militants d'Emmanuel Macron, et tant d'autres. Dans les tranchées du code, l'élément humain reste déterminant.

La certitude, forgée au fur et à mesure de la rédaction de cette enquête, que la technique seule était impuissante, et que l'humain restait déterminant, même dans le cyberespace, a renforcé notre confiance dans le seul outil que nous connaissons : le carnet de notes. C'est par une investigation tout à fait classique, faite de rencontres inopinées, de lecture frénétique et de moments de découragement intense, que nous avons pu remonter la piste des artisans de la fuite massive, et non par une contre-enquête informatique… Face au tsunami des fuites et à la normalisation du scandale, il nous paraît plus important que jamais de ne pas s'arrêter aux apparences, de ne pas considérer comme normal et évident ce qui est manifestement construit et scénarisé, de toujours chercher comment naissent et procèdent les fuites, bref de ne rien considérer comme sacré, ni les secrets d'État ni les serments moraux des *hacktivistes*. D'essayer, en

somme, d’être journaliste dans un monde hystérisé par ces armes de déstabilisation massive.

50 nuances de « leaks » : douze ans de fuites massives

Nous sommes à l'âge de la fuite. Pour s'en convaincre, il suffit de consulter la liste, forcément partielle, établie ci-dessous : depuis 2005, on ne recense pas moins de trente-cinq publications de bases de données confidentielles. Et le phénomène s'accélère : occasionnelle jusqu'en 2010, la fuite massive est désormais systématique. Entre 2015 et 2016, on ne compte pas moins de quinze divulgations de données protégées, soit près d'une tous les deux mois.

Ces publications sont systématiquement anonymes, à une seule exception près, celle d'Edward Snowden. Elles passent également toutes par Internet : les cas de transmission directe d'informations privilégiées à des journalistes représentent moins de 10 % des incidents recensés ci-dessous.

Sur le marché de la fuite massive, WikiLeaks est incontestablement l'organisation la plus active : la plate-forme de Julian Assange a mené à elle seule dix publications de bases de données confidentielles depuis sa création en 2006, dont cinq entre 2010 et 2012. Depuis, son rayonnement va décroissant, et le site s'apparente aujourd'hui à une vaste bibliothèque de documents confidentiels : WikiLeaks agrège toutes les données publiées ailleurs, souvent sur des sites éphémères, et les présente de manière accessible.

2005 :

Publication des noms de 276 agents du MI6, le service de renseignement extérieur britannique. Plateforme : cryptome.org

2008 :

Novembre : publication de centaines de documents internes de la filiale de la banque suisse Julius Baer aux îles Caïmans. Plateforme : WikiLeaks.

2010

Juillet : publication de 91 000 rapports de mission d'unités militaires américaines en Afghanistan. Plateforme : WikiLeaks.

Octobre : publication de 391 832 rapports de mission d'unités militaires américaines en Irak. Plateforme : WikiLeaks.

Novembre : publication de 251 287 télégrammes diplomatiques américains. Plateforme : WikiLeaks.

2011

Janvier : publication des documents de travail du négociateur de l'Autorité palestinienne Sa'eb Erekat. Plateforme : Al-Jazeera.

Février : publication de la messagerie de la société de sécurité informatique HBGary. Plate-forme : Project PM. Reprise en 2015 sur WikiLeaks.

2012

Février : publication des messageries de la société d'analyse géopolitique Stratfor. Plate-forme : WikiLeaks.

Juillet : publication de la messagerie de plusieurs hauts fonctionnaires syriens. Plateforme : WikiLeaks.

2013

Février : publication des messageries internes au groupe minier International Mineral Resources. Plateforme : *Harper's*.

Juin : publication de documents internes à la National Security Agency dupliqués par Edward Snowden. Plateforme : *The Guardian*, *The Washington Post* et, plus tard, *The Intercept*.

2014

Août : publication de la messagerie du ministre-conseiller de l'ambassade kazakhe en France Jean Galiev. Plateforme : Kazaword.

Novembre : publication de documents internes à l'antenne luxembourgeoise de PriceWaterHouseCoopers. Plateforme : International Consortium of Investigative Journalists.

2015

Avril : publication des messageries internes de Sony. Plate-forme : site Internet éphémère. Publication reprise par le magazine *Variety*, puis, plus tard, par WikiLeaks.

Juin : publication des messageries internes de la diplomatie saoudienne. Plateforme : le site éphémère Wikisaleaks. Publication reprise en novembre par WikiLeaks.

Juillet : publication des messageries de la société italienne Hacking Team. Plateforme : site éphémère, Bit Torrent. Publication reprise plus tard par WikiLeaks.

Juillet : publication de listes de personnalités françaises, allemandes et japonaises à surveiller, établies par la National Security Agency, l'agence d'interception américaine. Plateforme : WikiLeaks.

Août : publication des messageries internes du conglomérat indien Essar. Plateforme : Center for Public Interest Litigation.

Octobre : publication de la messagerie personnelle de John Brennan, alors directeur de la CIA. Plateforme : WikiLeaks.

Novembre : publication de guides de pilotage de drones armés américains. Plateforme : *The Intercept*.

2016

Avril : publication de 11,5 millions de documents internes au cabinet panaméen d'incorporation de sociétés offshore Mossack Fonseca. Plate-forme : International Consortium of Investigative Journalists.

Juillet : publication des messageries internes de l'AKP, le parti du président turc Recep Tayyip Erdoğan. Plateforme : site éphémère. Publication reprise par WikiLeaks.

Septembre : publication de la messagerie de l'ancien directeur général de la sécurité intérieure français, Bernard Squarcini. Plateforme : Kazaword.

Septembre : publication de la messagerie du courtier aéronautique américain Farhad Azima. Plateforme : site éphémère sur le réseau Bit Torrent.

Septembre : publication de la messagerie de Berat Albayrak, ministre turc de l'Énergie et gendre du président Recep Tayyip Erdoğan. Plateforme : site éphémère Dropbox. Publication reprise en décembre par WikiLeaks.

Octobre : publication de la messagerie de Vladislav Surkov, conseiller du Kremlin sur l'Ukraine. Plateforme : compte Twitter du groupe de hackers CyberHunta.

Décembre : publication des messageries internes du fonds d'investissement sportif Doyen. Plate-forme : European Investigative Collaboration.

Décembre : publication de documents internes de l’Église de Jésus-Christ des saints des derniers jours. Plateforme : Mormon Leaks.

2017

Février : publication de documents internes de la CIA sur l’élection présidentielle française de 2012. Plateforme : WikiLeaks.

Mars-août : publication des guides d’utilisation de dizaines de logiciels de surveillance et de capture d’information utilisés par l’Office of Technical Services de la CIA. Plateforme : WikiLeaks.

Mai : publication des messageries du parti En marche ! d’Emmanuel Macron. Plateforme : 4chan. Publication reprise en juillet par WikiLeaks.

Juin : publication de la messagerie de Yousef al-Otaiba, ambassadeur des Émirats arabes unis aux États-Unis. Plateforme : site Internet éphémère Bit Torrent.

Juin : publication de 200 000 e-mails internes au groupe Gupta, une dynastie d’affaires sud-africaine d’origine indienne. Plateforme : GuptaLeaks.com, un site mis en place par les médias sud-africains Daily Maverick et News24.

Août : publication d’e-mails internes au cabinet d’avocats portugais PLJM, dont le principal client est la fille du président angolais, Isabel dos Santos. Plateforme : European Investigative Collaboration.

En couverture : © Shutterstock
Création graphique : Nuits de Chine
Conception graphique : Antoine du Payrat

Dépôt légal : novembre 2017

© Librairie Arthème Fayard, 2017.

ISBN : 978-2-213-70676-4

Table

Couverture

Page de titre

I. – Les intrigants

Complot électronique dans les palais kazakhs

Confidences londoniennes

Squarcini éclaboussé par les fuites

Le mystère Rajat

Quand des données volées deviennent des armes judiciaires

Leçon de piratage

La loyauté à géométrie variable des hackers

II. – Les cambrioleurs

Tel Aviv, terre promise du hack

Les cyberespions de l'État hébreu

Genèse des stratégies électroniques israéliennes

Le bureau des cyberlégendes

New Delhi, le nirvana du hacking

L'État indien à la conquête de l'Internet

III. – Les stratèges

Instrument de déstabilisation politique

Les hackers, bras armés du Kremlin

Tableau de chasse de Fancy Bear

WikiLeaks et la Russie

Les lanceurs d'alerte de Poutine

Cyberingérence à Malte

IV. – Géopolitique de la fuite massive

Comment l'Iran a mis à genoux la diplomatie saoudienne

Guérilla électronique entre monarchies du Golfe

La Corée du Nord à l'assaut de Hollywood

Macronleaks, ou la déstabilisation à portée de tous

V. – Les receleurs

Les tribunaux lavent plus blanc

Cybercommandos judiciaires

Le tribunal mondial d'Internet

Fuites et contre-fuites

Intrigues dans le cybervillage

Hacking team : duel au (cyber)soleil

Chantage à la donnée

Profession : cybermercenaire

VI. – Les blanchisseurs

Les porte-étendards de la fuite massive

L'anonymat : un bouclier ou une arme ?

La contre-histoire de WikiLeaks

La fuite massive, drogue dure des médias

Responsables, mais pas coupables

Les journalistes, agents de déstabilisation à leur insu ?

VII. – Les profiteurs

La cyberconjuration de Team Themis

Sus au Darknet

Traquer ses propres employés, un marché d'avenir

Épilogue

Page de copyright

Notes

1. « On évoque sans cesse la technologie, mais notre meilleure protection n’est pas la technologie ; notre meilleure protection, ce sont des hommes et des femmes motivés, agiles et capables d’anticiper et d’innover. Car, en face, il y a aussi des hommes et des femmes, assis devant leur ordinateur quelque part dans le monde. Il y a une dimension humaine dans tout ceci. Il ne s’agit pas seulement de machines. »

This file was downloaded from Z-Library project

Your gateway to knowledge and culture. Accessible for everyone.

z-library.sk z-lib.gs z-lib.fm go-to-library.sk

Official Telegram channel

Z-Access

https://wikipedia.org/wiki/Z-Library